FACULTAD DE COMERCIO
Universidad de Valladolid

GRADO EN COMERCIO

TRABAJO FIN DE GRADO

Seguridad en las compras online

César De Juan Guerra

FACULTAD DE COMERCIO
VALLADOLID, FECHA

FACULTAD DE COMERCIO
Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID

GRADO EN COMERCIO

CURSO ACADÉMICO 2022-2023

TRABAJO FIN DE GRADO

“Seguridad en las compras online”

Trabajo presentado por: César De Juan Guerra

Tutor: Francisco Javier Galán Simón

FACULTAD DE COMERCIO
Valladolid, julio 2023

Contenidos

Listado de gráficos

Listado de gráficos

Listado de imágenes

1. Introducción

El comercio electrónico se puede definir como el proceso de compra de información, bienes y servicios entre consumidores y empresas, a través de internet. En este tipo de comercio se puede encontrar diferentes actividades como servicios de suscripción streaming, subastas, transacciones comerciales electrónicas, etc. La facilidad y la comodidad que ofrecen este tipo de comercio son sus puntos fuertes en la decisión de los consumidores, también es importante destacar que este puede realizarse en cualquier parte del mundo desde cualquier dispositivo electrónico, ya sea ordenadores o smartphones.

Para hablar de la evolución del comercio electrónico hasta la actualidad debemos remontarnos a 1920 donde en Estados Unidos se realizan las primeras ventas por catálogo las cuales se asemejan al comercio electrónico. Más tarde surge el teléfono y la EDI (Electronic Data Interchange) gracias a la cual se transmitían órdenes, datos y facturas de manera electrónica.

En 1970 Michael Aldrich ejecuta las primeras transacciones electrónicas de venta en la década de los 90 aparecieron las plataformas de comercio virtual como Amazon, eBay y Mercado libre, más tarde la National Science Foundation eliminó las restricciones de internet para su uso comercial ampliando así su capacidad para comercializar. En 1992 se crea el IBM Simon, conocido actualmente como el primer smartphone de la historia, distribuido por los Estados Unidos.

Este dispositivo conocido también como "Simon de Comunicación Personal" o "Teléfono Inteligente IBM Simon", no solo daba las prestaciones de un teléfono móvil, sino que también funcionaba atributos propios de una PC en un dispositivo portátil. También, fue el primer dispositivo móvil que tenía un panel táctil y permitía el envío de textos. Tenía un panel táctil con una medida de 4.5 pulgadas, lo que lo volvía revolucionario para la época. También, tenía una GUI que les permitía a los usuarios desplazarse por diferentes apps y opciones fácilmente.

Entre las características destacaban en el IBM Simon la capacidad de enviar y recibir correos electrónicos, hacer llamadas telefónicas, enviar mensajes de texto, organizar contactos y gestionar tareas de calendario. Asimismo, se le atribuyó la aptitud de enviar y recibir documentos fax. También, era capaz de hacer apuntes y avisos, lo que significa que lo hacía una herramienta adaptable en aquel entonces.

No obstante, es necesario mencionar que, a pesar de ser innovador y tener una perspectiva de futuro, el IBM Simon no logró un gran éxito en el mercado. La complejidad extrema y el alto precio obstaculizaron su adopción generalizada desde el público. No ocurrió hasta mucho tiempo después, a medida que la tecnología avanzaba y la llegada de sistemas operativos más amigables y accesibles. En el momento en que los celulares se hicieron populares en todas partes.

Figura 1: Ejemplo de IBM Simon. Fuente: EL ESPAÑOL (2016)

En ese mismo año el navegador web Netscape implementó el protocolo SSL (Secure Sockets Layer) el cual permitía la transmisión de datos privados de forma segura. En 1998 se funda PayPal, el cual ofrece a los usuarios un pago electrónico seguro y fiable lo cual incrementó la confianza en el comercio electrónico. En los años 200 Google crea también su forma de pago llamado Google Checkout además del nacimiento de eventos Cyber los cuales generaban grandes descuentos para fomentar las compras de manera online. En 2014 se produjo un incremento muy acelerado de las ventas electrónicas y en 2020 debido a la pandemia causada por el COVID-19 dio como resultado un boom en el comercio electrónico ya que según Daterportal en julio de este año el 71% de personas en el mundo confirmó hacer compras digitales.

Al hablar del comercio electrónico tenemos que distinguir tres tipos; el realizado entre consumidores llamado *Consumer to Consumer (C2C),* otro tipo sería el que realizan

entre empresas, Business *to Business* (B2B) y por último el tipo más común el cual se hace entre empresa y consumidor, se denomina *Business to Consumer* (B2C).

Muchas son las ventajas que podemos encontrar en el comercio electrónico, sin embargo, las desventajas y sobre todo las amenazas que puedan sufrir los consumidores y las empresas pueden ser mucho más impactantes y dañinas. El fraude es el delito electrónico más común entre el comercio digital, afecta tanto a consumidores como a empresas, vulnerando su información personal y financiera, sus datos de contacto y su confianza por este tipo de comercio.

Por ello es importante poner en conocimiento a los usuarios, tanto empresas como consumidores, las medidas y protocolos de seguridad que deben tomar para reducir lo mínimo posible el riesgo de caer en alguno de estos tipos de fraudes electrónicos y protegiendo así su información personal y financiera lo máximo posible.

1.1 Justificación

Como he mencionado anteriormente el comercio electrónico se ha convertido en un mercado importante para los consumidores a la hora de comprar de productos y servicios en los últimos años. Al padecer dicho auge también ha generado una mayor importancia la seguridad sobre todo cuando se trata de compras online.

El fraude online cobra una gran inquietud por parte de los consumidores debido a que la información personal y financiera puede ser los principales objetivos de ciberdelincuentes en páginas maliciosas o a través del método phishing. Las transacciones online pueden ser afectadas por diversos problemas de carácter técnico, así como problemas en la conexión o en el procesamiento de un servicio lo cual puede derivar a la pérdida de datos.

En España este tipo de comercio aumentó en 2020 un 21,7%, según la Cámara de Comercio de España. El mayor uso de comercio digital ha resultado en un aumento de los delitos online, no obstante, debido a este aumento de la delincuencia se han tomado un mayor uso de medidas de seguridad para proteger a los consumidores de todo tipo de amenazas que pueden causarles fraudes o robos de identidad y datos personales. Por ello es importante cerciorarse de la protección que brindan las tiendas digitales además de tomar las medidas de seguridad propias como instalar y actualizar antivirus y elegir contraseñas muy seguras. Además, el papel de las empresas cobra mucha importancia ya que deben garantizar la seguridad de sus consumidores a la hora de realizar ventas de forma online.

La ciberseguridad es clave para garantizar los beneficios del comercio a los consumidores de la forma más segura posible. Es importante abordar este tema para que los consumidores se informen y tengan los conocimientos necesarios para protegerse y que por parte de las empresas vendedoras sean las responsables de usar medidas efectivas de seguridad para proteger y seguir manteniendo la confianza del factor más vulnerable: los consumidores.

1.2 Justificación del estudio

La justificación de la realización de este trabajo es entender y plantear los diferentes problemas de seguridad online, ya que si hablamos de economía online la seguridad es un concepto que anualmente está cobrando mayor importancia. Al haber aumentado el número de transacciones económicas en el comercio electrónico ha derivado en un mayor movimiento de datos financieros y personales, los cuales son vulnerables a ser robados y utilizados con mala fe. Ambas partes del acuerdo (las compañías y los clientes) aprecian mucho la seguridad como factor clave. Este ofrece un servicio fiable en su portal web. La falta de confianza expresada por los usuarios se transforma en una barrera al efectuar compras o adquirir servicios. Esto tiene efectos adversos en los negocios tanto desde el punto de vista monetario como en su credibilidad.

El factor crucial en este estudio consiste en evaluar los riesgos potenciales que perjudican a los usuarios durante las transacciones online. También, se intenta crear conciencia acerca de las precauciones y reglas de seguridad que pueden resolver o prever estos problemas. Mediante esta labor, busco informar a los consumidores acerca de las precauciones fundamentales que deben considerar al realizar compras por Internet y así disminuir cualquier posible riesgo.

A mi juicio, es crucial realizar este trabajo para brindar información y generar consciencia acerca de la ciberseguridad debido a su gran importancia en el comercio electrónico.

1.3 Objetivos de la investigación

El principal objetivo de esta investigación es analizar los problemas de seguridad es analizar y dar a conocer los distintos problemas de seguridad digital además de poner en conocimiento a consumidores y empresas las medidas más efectivas para reducir al mínimo posible el riesgo de fraudes digitales y garantizar al máximo la seguridad en línea. Para poder alcanzar el objetivo principal se presentan los siguientes objetivos específicos:

1. Realizar análisis de los principales riesgos y amenazas que afectan a los consumidores y las empresas cuando se hacen compras en línea además de conocer los puntos débiles donde puede verse afectado la el comercio entre empresa y consumidor.
2. Evaluar la efectividad de los mecanismos de protección aplicados en las medidas de seguridad elegidas, así como comprender cuáles son los aspectos fuertes y débiles al comprar en línea. Gracias a estos conocimientos obtenidos podemos otorgar recomendaciones y estrategias al consumidor y empresas para reducir el riesgo de fraude.
3. Realizar análisis de control de las recomendaciones y mecanismos implementados, así como la rentabilidad e imagen de la empresa vendedora de bienes y servicios el cual tiene la capacidad de generar mayor confianza en el consumidor. Dependiendo de los resultados obtenidos se puede mantener u optar por otras medidas que garanticen la seguridad y la protección del consumidor.

Con esto se busca asegurar un entorno protegido y fiable para contribuir con el crecimiento del comercio electrónico.

1.4 Hipótesis

La hipótesis de este trabajo se fundamenta en que, dado que se presentan múltiples riesgos y amenazas que se ubican en el comercio electrónico, es posible utilizar varias estrategias y mecanismos de resguardo para disminuir la oportunidad de que se presente toda clase de estafa financiera, robo de identidad o fraude. Por eso, la seguridad es indispensable y básica para los consumidores.

Es posible destacar diferentes métodos que garantizan la seguridad de los clientes. Por instancia, la configuración de conexiones seguras con protocolos encriptados y la verificación del vendedor en el sitio web. Además, es fundamental concienciar a los usuarios respecto a los peligros cuando se compra algo en internet. También, es crucial colaborar en la identificación de peligros o páginas falsas.

Además, el avance de estas iniciativas traerá beneficios para las firmas de distribución. Aumentarán la protección de los clientes y mejorarán la felicidad de los consumidores, sustentando una apariencia de marca intachable y admirada. Preservar un lugar seguro permitirá que el comercio en línea sea una opción atractiva y fácil de usar para los usuarios. Esto ayudará al amplio uso de la compra en línea. Con este supuesto, se busca probar que la implementación de medidas de seguridad adecuadas puede resultar en un balance positivo entre la seguridad y la experiencia del usuario además de producir una confianza adicional en los consumidores y fomentar la marca de la tienda web.

2 Marco teórico

Este trabajo de fin de grado tiene como objetivo presentar el conocimiento básico sobre la seguridad en compras online. Para ello se ha realizado una investigación por medio de fuentes de información y estudios académicos para conocer los puntos claves de este campo y otorgar a los consumidores las distintas medidas y estrategias de seguridad para proteger su información personal y financiera.

Primero, se presentará el inicio del comercio electrónico así también los diferentes tipos de eCommerce que se encuentran en internet. Se dará a conocer las medidas más eficaces para realizar compras online de forma segura, así como conocer los protocolos que las tiendas utilizan para asegurar su sitio web. Mediante la recopilación de información se buscará informar a los usuarios cuales son las distintas amenazas y riesgos que pueden sufrir mientras compran de forma online y cuáles son las consecuencias de estas.

Además, se enseñarán las normativas y regulaciones que envuelven al comercio electrónico, así como, las diferentes leyes que regulan y protegen de delitos a este tipo de comercio.

Por último, se llevará a cabo una investigación de naturaleza cualitativa para comprobar la hipótesis ya mencionada. Este análisis se basará mediante una encuesta constituida por 16 preguntas. Estas consultas fueron creadas para indagar la comprensión y las medidas de seguridad que las personas siguen al efectuar compras electrónicas. Con los datos extraídos del cuestionario, se llevará a cabo realizar un examen. A partir de esta evaluación, se logrará una deducción acerca de los propósitos deseados.

2.1 Comercio electrónico

El mercado de bienes y servicios por internet es una forma muy común para adquirir todo tipo de productos en los tiempos recientes. No obstante, resulta fundamental ser cauteloso cuando se hacen compras por internet y cerciorarse de que se está usando un sitio web seguro y confiable. Todos los años este tipo de adquisiciones de productos y servicios se transforman utilizando todo tipo de vías para efectuar intercambios monetarios. Ya sea mediante teléfonos móviles, plataformas sociales, equipos informáticos, y otros, es un método rápido para obtener bienes y servicios con gran facilidad y accesibilidad. Del mismo modo el negocio electrónico proporciona a las empresas una forma de venta eficiente y enormemente rentable entre un público global. Este tipo de negocio se puede dividir en los siguientes tipos de comercio:

- B2B (Business to Business): Este tipo de negocio involucra intercambios comerciales efectuados exclusivamente entre compañías. En esta situación, las compañías operan además de proveedores en calidad de clientes. Trocan artículos, prestaciones o datos entre ellos. Este estilo de venta en línea es fundamental en el mundo de los negocios. Incluye una amplio abanico de campos y segmentos. Por instancia, una compañía tecnológica que comercializa piezas a otras firmas de electrónica ejemplifica de manera clara un enfoque B2B.

- B2C (Business to Consumer): En este enfoque comercial, se realizan las transacciones entre compañías y clientes. En este lugar, las compañías ejercen como vendedoras, brindando productos o servicios sin intermediarios al usuario. Este representa uno de los principales modelos más populares en el comercio digital. Implica a los establecimientos virtuales y sitios web de compras que dan a conocer productos y servicios directamente al público en general. Por instancia, un comercio electrónico de prendas de vestir que ofrece sus mercancías a los clientes últimos aplica la estrategia B2C.

- C2C (Consumer to Consumer): En esta situación, los consumidores realizan transacciones electrónicas entre sí. Las personas usan sitios web o espacios de comercio online para ofrecer artículos o prestaciones a otros compradores. Un caso típico de este sistema es una herramienta de remates en la web. Los clientes pueden ofrecer para la venta sus mercancías para que otros clientes los

obtengan. Además podríamos referir las plataformas de adquisición y comercialización de productos usados. En estos plataformas, las personas transaccionan y adquieren artículos entre ellos.

- C2B (Consumer to Business): Este enfoque es poco habitual y requiere una inversión de la metodología tradicional. En este lugar, los clientes son que brindan sus artículos o servicios a las entidades.

Figura 2: Tipos de e-Commerce Fuente: FacturaCión (2020)

Garantizar la protección es una prioridad fundamental cuando se realiza movimientos económicos en la web. Podemos encontrar diferentes formas de estafas como el hurto o el fraude de identidad, la estafa o la existencia de software malintencionado en el sitio web. Los métodos y normas de seguridad deben estar eficientes para garantizar el resguardo de los registros de los consumidores. No obstante, también se debe destacar asegurar el acceso y la accesibilidad de los datos si es necesario.

Las estrategias y acciones más comunes en el sector de las transacciones digitales implican la encriptación de información a través de certificados SSL (Secure Sockets Layer), verificación de identidad con múltiples factores, herramientas para

identificar fraudes, políticas de confidencialidad, proteger información personal, etc. Asimismo, es esencial considerar que cada nación define sus propias orientaciones y disposiciones en el sector del comercio en línea. Entre estas normas y normativas se admite la responsabilidad de la empresa o el distribuidor y el consumidor en las operaciones en línea. No obstante, además se establece la carga del consumidor de asegurar sus datos de identidad y bancarios.

Por lo tanto, las personas involucradas en una transacción económica deben considerar los diferentes peligros que pueden surgir. Igualmente, las entidades deben procurar prevenir riesgos o peligros que dañen a los usuarios y, para lograr ese propósito, ejecutar las medidas adecuadas. También, resulta crucial que los clientes conozcan y comprendan detectar fraudes que puedan causarles daño de alguna manera u otra.

2.2 Seguridad en compras online

En el mundo tecnológico que actualmente vivimos, las ventas en línea han padecido un aumento muy acelerado. Esto ha cambiado el modo en que los seres humanos realizan compras de bienes y servicios. Este tipo de adquisición, que se lleva a cabo mediante sitios web, brinda una extensa selección de beneficios y conveniencias para los clientes. Les posibilita comprar artículos desde sus casas y poder alcanzar un catálogo global sin restricciones geográficas. No obstante, este crecimiento de las compras en línea también ha traído problemas vinculados a la protección de los datos personales y financieros. En consecuencia, se requiere llevar a cabo acciones complementarias con el fin de asegurar la privacidad y la exactitud de los datos enviados vía plataformas digitales.

La protección en las transacciones en línea se ha transformado en una preocupación primordial para ambas partes. Toda compra por internet se puede enfrentar a múltiples peligros y riesgos, como el hurto de identidad, el engaño económico o la entrada sin permiso a datos sensibles. La seguridad de los clientes es fundamental esencial para la victoria de toda empresa en internet. La seguridad de un ambiente protegido y resguardado es fundamental para estimular conexiones duraderas con los consumidores.

En esta situación, el presente estudio tiene como propósito indagar y entender la opinión y el saber de los usuarios con respecto a la protección en las compras en línea. Por ello se busca recopilar datos importantes acerca de cómo los consumidores aprecian

la protección de las transacciones económicas en línea. Por otra parte, concienciar sobre la importancia de las normas de protección y las situaciones de riesgo a las que los clientes pueden estar expuestos es fundamental para garantizar un tipo de mercado seguro y cómodo.

2.2.1 Términos y condiciones

La legislación de protección de datos, la normativa de servicios de pago, los reglamentos de seguridad de la información y la red y la normativa de comercio electrónico representan reglamentos y normas que garantizan la seguridad en el comercio electrónico. Estas leyes y reglas protegen los datos personales de manera efectiva, la protección de las operaciones financieras, la seguridad de los datos en Internet y la observancia de las normativas del comercio digital.

Las compañías deben seguir las exigencias definidas por este conjunto de reglas para proteger el bienestar de los compradores. Además, es necesario proteger la información personal y financiera, e informar sobre posibles infracciones de seguridad, acontecimientos, validación de movimientos monetarios y el deber de notificar a los clientes las medidas de protección.

Hay varias entidades responsables de garantizar la protección del comercio en internet. Una de las opciones es el estándar ISO 27001, que define lineamientos para los sistemas de seguridad informática.

La ISO 27001 establece de manera internacional los requisitos para poder implementar, mejorar y mantener el SGI (Sistema de Gestión se la Seguridad de la Información). Este estándar se implementa en todo tipo de organizaciones ya sean grandes, medianas o pequeñas empresas, en instituciones públicas y gubernamentales o en sectores públicos, tecnológicos y relacionados con la salud. (*¿Qué Es La Norma ISO 27001 Y Para Qué Sirve?* | *GSS*, 2023)

2.2.2 Amenazas y riesgos

Hay muchos peligros y riesgos relacionados con las compras electrónicas. Algunos de aquellos involucran el robo de identidad, la estafa online, el fraude, el saqueo

de datos personales y financieros, entre otras cosas.

La estafa en línea representa un desafío frecuente en las transacciones en línea. Los criminales pueden adquirir datos personales y de dinero de los usuarios para llevar a cabo fraudes en línea. La estafa de phishing es una táctica más utilizada por los infractores para obtener información personal del comprador usando correos electrónicos engañosos. Estas comunicaciones electrónicas incluyen vínculos a páginas web fraudulentas o imaginarias que aparentan ser auténticas. Sin embargo, conversamos sobre uno de los más grandes riesgos que los usuarios pueden encontrar en la red.

El fraude por falsificación de datos personales, uso de tarjetas de crédito robadas o sitios web clonados es más común en el comercio electrónico. La privacidad y seguridad de la información personal es otro factor de riesgo en las compras en línea.

Varios sitios web que ofrecen productos o servicios recogen información confidencial de sus clientes. Esta información engloba datos referentes a las modalidades de pago utilizadas o los detalles de contacto proporcionados por los usuarios. Desafortunadamente, esta información se puede usar con objetivos no deseados. Otra estrategia para realizar fraude dirigido a los consumidores es la suplantación de identidad. La técnica de phishing consiste en métodos empleados por los criminales para fingir ser una compañía, individuo u organización confiable. El propósito consiste en manipular y conseguir información personal, asimismo entrar a las cuentas bancarias de los usuarios.

Figura 3: 8 consejos para descubrir un correo de Phishing. Fuente: GLOBAL TECHNOLOGY (2023)

Aparte del phishing, es frecuente la obtención de archivos maliciosos que pueden comprometer la protección de los dispositivos electrónicos y datos personales del usuario. No obstante, se pueden tomar precauciones que se pueden ejecutar para asegurarse contra estas amenazas. El transporte de la adquisición efectuada tiene la posibilidad de ser una fuente de riesgo. Los datos personales de la mercancía y los datos de transacción pueden ser sustraídos durante el envío del producto.

Frente a los peligros mencionados que perjudican el comercio digital, las compañías y los clientes deben adquirir los conocimientos adecuados para resguardarse y aplicar medidas de protección en las transacciones monetarias que realizaron. De la misma manera que tener la capacidad de descubrirlo oportunamente cuando sea viable.

Las precauciones de seguridad implementadas por ambos lados llevarán a un lugar seguro y confiable. También, se permitirá la capacidad de progreso del comercio en internet.

2.2.3 Medidas de seguridad

Como se dijo antes, las políticas de seguridad son elementos vitales para la protección, seguridad, privacidad y confianza del usuario. No obstante, también es fundamental resaltar que es necesario mantener y mejorar constantemente estos sistemas para enfrentar los nuevos riesgos y retos que emergen en el contexto digital. Sin embargo, también es importante destacar que es importante mantenerse actualizado y mejorar estas acciones de manera constante para responder a los nuevos riesgos y desafíos tecnológicos. No obstante, es necesario resaltar que es esencial mantener estas actualizaciones y mejoras de forma constante para hacer frente a los nuevos desafíos y riesgos tecnológicos. También es relevante mencionar que es fundamental actualizar y mejorar constantemente estos procedimientos para enfrentar los nuevos riesgos y desafíos tecnológicos.

Hay que tener en cuenta que resulta crucial tener presente que la seguridad nunca será un propósito final, sino una evolución continua de adaptación y mejora continua. Sin

embargo, es importante destacar que las transformaciones y mejoras deben efectuarse continuamente para hacer frente a los riesgos y retos tecnológicos emergentes.

Estos pasos deben ser llevados a cabo por compañías y clientes. Por ende, deben tener conciencia de las posibles amenazas que pueden impactar a sus compras en línea. Los usuarios deben poseer la información fundamental para poder reconocer los peligros presentes en las compras en línea y realizar acciones para disminuir al máximo los engaños. Las medidas de seguridad implican escoger un sitio seguro y seguro.

También, es importante analizar las reglas de protección de datos del sitio web. Utilizar claves altamente confiables y asegurar la seguridad de las transacciones económicas mediante medidas de protección. Las compañías que suministran mercaderías y apoyo en la web deben asegurar la seguridad de los consumidores durante las transacciones con ellos. Asimismo, resulta crucial que proporcionen protocolos de seguridad apropiados para asegurar la información privada y económica de los consumidores. Esto mismo se logra mediante por medio de pruebas de la protección en el sitio en internet. Asimismo, se comprueba la autenticidad del comprador y se emplea cifrado para la información personal de los clientes, entre otras medidas de seguridad.

Después, se presentan las mejores medidas de seguridad preventivas que impidan que el consumidor sufra las repercusiones de los peligros que pueden encontrarse en las compras en internet, conforme al artículo ("Compra segura en INTERNET".):

1. La utilización de un programa antivirus completo asegura la seguridad al descargar archivos, la eliminación y las capacidades de aviso de amenazas de virus que podrían perjudicar a los usuarios. Algunos programas antivirus son resistentes al phishing y a posibles ataques de piratería en dispositivos electrónicos.
2. Realizar actualizaciones a los dispositivos electrónicos: Tanto los dispositivos como los sistemas operativos que integran pueden ser débiles a amenazas de seguridad por no estar actualizados. Muchas de las actualizaciones mejoran la versión anterior corrigiendo los errores de seguridad que puedan tener. Por ello mantener los dispositivos actualizados es uno de los puntos más importantes que el usuario debe tener en cuenta para su seguridad y para estar protegido.

3. Evite utilizar aparatos electrónicos en lugares públicos: La ausencia de actualización de los aparatos, el acceso a redes inalámbricas públicas o la carencia de seguridad al explorar en Internet a causa de malware puede haber varias causas por las que los datos no se encuentran disponibles. Estos casos afectan la confidencialidad y el dinero del cliente.
4. Se recomienda a las personas que creen claves que tengan diferentes símbolos. Esto implica caracteres en mayúscula, símbolos especiales y números. Además, no debería emplear la misma password en todas las aplicaciones. Los datos personales y económicos pueden estar expuestos a la ciberdelincuencia e intrusiones no permitidas. Proteger la imagen del comercio electrónico es crucial cuando se trata de llevar a cabo una compra en el mundo virtual. Para conseguirlo, es esencial informarse acerca de la vivencia de otros usuarios, informarse sobre las precauciones de seguridad que la tienda implemente e informarse sobre la excelencia de los servicios que brinda. Así, es posible prevenir engaños y sustracciones de datos personales.

A continuación, se expondrá una imagen con ejemplos de recomendaciones que debe tomar el usuario en el momento de realizar una compra por internet.

Figura 4: Recomendaciones para realizar compras seguras en internet Fuente: Ministerio de Consumo (2020)

Además, los negocios tienen la responsabilidad de verificar un ambiente seguro, sin amenazas ni riesgos para sus clientes. A continuación, se van a nombrar los diferentes métodos y protocolos de seguridad que las empresas implementan en sus tiendas online: (“Compra segura en INTERNET”)

1. Certificados de capa de servidor segura (SSL): Este tipo de protocolo consiste en la utilización de un sistema cifrado entre el servidor web y el usuario. Gracias a este cifrado los datos del cifrado se encuentran protegidos y garantiza una navegación segura. Para saber si una página web está protegida mediante el certificado de capa de servidor segura (SSL) debemos observar la URL y si esta empieza por “https://” mientras que si la URL comienzo por “http://” quiere decir que ese servidor web no está protegido mediante un certificado (SSL). También puede encontrar un candado para asegurarse de que esta página está protegida por este protocolo de seguridad.

Figura 5: URL de ejemplo con certificado de servidor seguro. Fuente: Elaboración propia

2. Cortafuegos (Firewall): Es un sistema de seguridad informática, también llamado firewall en inglés, que se implementa en equipos informáticos y redes para protegerlos contra posibles amenazas y accesos no autorizados desde el exterior. Opera como un obstáculo en medio de una red privada o cualquier dispositivo realizando su función la cual es regular el flujo de información que ingresa y sale, asegurando de esta manera la protección y la confidencialidad de la red o del equipo. Esto se realiza autorizando o denegando la entrada según los requisitos de seguridad predefinidos. Estos principios pueden ser ajustados por el encargado del sistema para definir qué clases de conexiones y servicios se aceptan. También, pueden decidir qué tienen que ser impedidos o descartados.

El firewall tiene la capacidad de funcionar en el nivel de los componentes, routers o equipos particulares. Asimismo, puede trabajar a nivel de programas en sistemas de ordenadores y software. Si un paquete de información intenta ingresar a la red o al dispositivo protegido, el firewall analiza el contenido del paquete y contrasta sus atributos con las normas establecidas. En caso de que el paquete respete los requisitos, se autoriza la entrada, si no respeta los requisitos se prohíbe el ingreso al paquete. En caso de que el paquete se ajuste a los términos estipulados, se autoriza su ingreso si es así, se detiene y se niega.

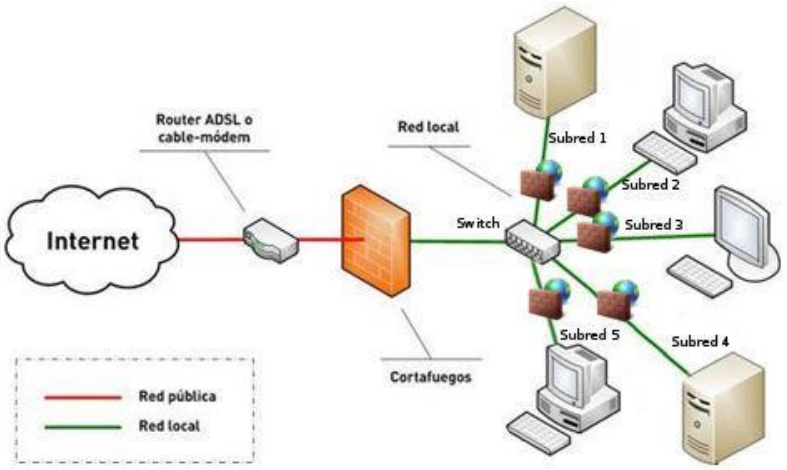

Figura 6: Ejemplo del funcionamiento de un cortafuegos. Fuente: geekland (2013)

Podemos destacar dos tipos de cortafuegos (firewall):

- Físico: Un firewall físico puede ser un dispositivo independiente o estar conectado directamente a su enrutador. Es relativamente fácil de usar, ya que puede ser muy efectivo para detectar amenazas o malware en su red sin mucha configuración. Estos cortafuegos constan de cuatro puertos para conexiones informáticas. Debido a que estos tipos operan a través de banda ancha, pueden manejar más datos y facilitar su trabajo porque puede controlar la seguridad de varias computadoras y páginas web con un solo dispositivo.

Figura 7: Ejemplo de cortafuegos físico. Fuente: geekland (2013)

- Lógico: Este tipo de cortafuegos lo ejecuta un programa instalado en el dispositivo. El programa puede permitir o denegar el acceso a Internet. Para aquellos usuarios que no tengan experiencia informática o de ciberseguridad este tipo de cortafuegos puede llegar a ser complicado ya que emite diversas alertas en cada acción realizada por el usuario.

3. Software antimalware: Esta medida de seguridad se basa en un tipo de software que identifica, elimina y protege al dispositivo de software malware. Se puede diferenciar del antivirus en que el antimalware está especializado en toda la gama de amenazas y de software malicioso mientras que el antivirus trabaja en proteger al dispositivo de un tipo de virus en específico por lo que es más eficiente para la seguridad del usuario el uso de antimalware. Podemos identificar distintos tipos de software dañino: (Acronis)

- Troyano: como sugiere el nombre, este tipo de malware parece un archivo, programa o código legítimo y seguro, pero hace exactamente lo contrario. Este tipo de malware se camufla y abre lagunas en su dispositivo sin su conocimiento, comprometiendo la seguridad de su dispositivo. Puede robar sus datos personales, espiarlo o inyectar otro malware. El nombre está relacionado con una pieza del caballo de Troya registrada en la Ilíada de Homero

- Virus: Es un tipo de malware que afecta, réplica o corrompe archivos y funcionalidades del dispositivo del usuario. Es el tipo de software malware menos común ya que solo representa el 10% de todos ellos. Uno de los

virus más comunes es el llamado adware (*Adware* | *INCIBE*, s. f.). Este virus informático se define como un software malware cuya función es mostrar al usuario publicidad no deseada o engañosa mediante una página web o un programa instalado con el objetivo de recibir algún tipo de beneficio económico.

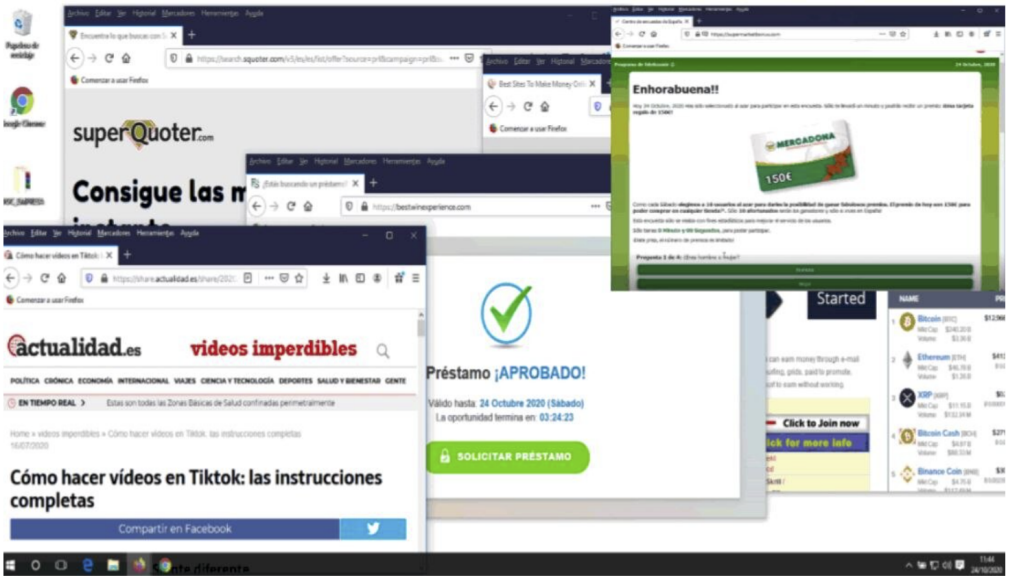

Figura 8: Ejemplo de ordenador infectado con “Adware” Fuente: BBVA (2020)

- Ransomware: Podemos catalogar este tipo de malware como uno de los más peligrosos para los usuarios. Ransomware toma el control de su dispositivo. En otras palabras, roba cualquier información personal que pueda haber en su ordenador o teléfono móvil. Se puede encontrar en archivos que aparentan ser legítimos como un correo electrónico o descargado de un enlace procedente de internet.
- El emisor de este malware pide un rescate, lo cual, el pago de este no asegura que se devuelva la información robada. Los procedimientos ante esto es hacer previamente una copia de seguridad, acudir a la policía y no ceder ante el chantaje ni pagar el rescate. A continuación, se mostrará una imagen con las medidas que tomar para evitar un ransomware y cómo actuar si han sufrido este tipo de malware.

Figura 9:Medidas para evitar ser víctima de “Ransomware” y cómo actuar. Fuente: Dataseg (2017)

- Puerta trasera (Backdoor): Podemos definir como puerta trasera como aquel punto de vulnerabilidad donde el delincuente puede acceder a una página o servidor web sorteando las barreras y medidas de seguridad programadas. Mediante este método, el atacante puede colocar un programa maligno, como un malware, gusano o spyware, impactando a esos sujetos que naveguen por la página web o descarguen una aplicación.

- Keylogger: El funcionamiento de esta aplicación se sustenta en identificar las pulsaciones que el usuario hace en su teclado. Además, asimismo almacena los sitios que explora, las pláticas privadas y su comportamiento

en línea. La función principal de este software malicioso consiste en descubrir los password de los usuarios y obtener acceso a datos personales y de cuentas bancarias. Este peligro puede perjudicar a distintos tipos de dispositivos electrónicos.

1. Requisitos de PCI-DSS: Es como un conjunto de métodos y medidas de seguridad que deben ser seguidas por todas las compañías que envían, procesan y transmiten datos de tarjetas de crédito o débito en su página de internet. Esto garantiza un ambiente seguro para las personas.

   El origen PCI-DSS se produjo en el año 2006. Durante ese año se fundó una entidad dedicada únicamente al desarrollo y establecimiento de estándares de seguridad en el sector de pagos con tarjeta. Esta propuesta fue apoyada y formada por las principales organizaciones del sector financiero. Ellas entendieron la imperante necesidad de proteger la seguridad y confidencialidad de los registros financieros de los clientes.

   La meta principal del estándar PCI-DSS consiste en asegurar la máxima seguridad y resguardo en las operaciones efectuadas por los consumidores por medio de las formas de pago plásticas, tanto crédito como débito. Esto es válido particularmente cuando se realizan compras a través de la web.

   Con el fin de lograr este objetivo, la empresa ha implementado un grupo de 12 condiciones esenciales que todas las compañías involucradas en el manejo de operaciones con tarjetas deben cumplir rigurosamente. Estas condiciones aseguran la protección y privacidad de los datos de los clientes reduciendo la posibilidad de sufrir una amenaza en sus compras online.

   Estas condiciones contienen varias precauciones de seguridad, iniciando con la colocación de firewalls y sistemas de encriptado, hasta la adhesión a políticas de acceso restringido y controles regulares para asegurar el cumplimiento de las pautas establecidas. También, se pretende asegurar la seguridad de los datos privados y la privacidad de los documentos.

   El cumplimiento de los estándares de seguridad de datos de tarjetas de pago no

solo protege a las personas que utilizan el servicio y sus datos económicos. Además refuerza la seguridad de los clientes en las transacciones electrónicas y estimula un entorno de comercio más seguro y confiable.

Estos requisitos son los siguientes:

Figura 10: Requisito de seguridad requeridos por PCI-SSC. Fuente: PCI Hispano (2022)

2.2.4 Normativas y regulaciones

Esta normativa define el modo en el que las organizaciones deben adquirir, almacenar y manejar la información personal de los clientes. Asimismo, incorpora sus datos económicos y de identificación. La falta de cumplimiento de las normas establecidas conlleva castigos financieros y legales cruciales para la empresa. A pesar de esto, en caso de que la empresa cumpla con el reglamento, se impedirán estas consecuencias negativas.

La normativa 2020/75/CE tiene como objetivo principal armonizar las normas que se aplican al comercio en línea en los países del bloque europeo. La meta se trata de

promover la libre circulación de prestaciones en línea. También, tiene como objetivo ofrecer una legislación clara y segura para los proveedores de servicios y los usuarios por igual.

La normativa 2013/2006 busca reconocer la autenticidad de las firmas en línea, estableciendo una comparación con las rúbricas manuales tradicionales. También, promueve la aplicación en los procesos y trámites digitales.El propósito consiste en promover la optimización y la protección en el mundo digital. (Ministerio de Consumo, s. f.)

Entre ellos, es importante mencionar, junto con la legislación específica de protección de los consumidores, los reglamentos de comercio interno, sobre todo las ventas por internet. Asimismo, se debe resaltar la normativa de la publicidad en general, y también la que incluya la publicidad y promoción de ciertos productos y servicios.

Además, es necesario considerar las diversas leyes relacionadas con la entrada, fabricación, cambio, conservación, traslado, reparto y utilización de los productos y servicios disponibles. Particularmente, es importante tener en cuenta las limitaciones en la venta de determinados artículos bajo ciertas circunstancias o la obligación de obtener permisos o registros. Entre estas leyes se encuentra: (Legislación Del Comercio Electrónico, s. f.)

1. *Legislación 7/1996* del 15 de enero, de Regulación del Comercio Minorista, BOE número. La meta fundamental de este estatuto consiste en establecer un conjunto de reglas que impulse la rivalidad justa entre diversas tiendas minoristas. Además, persigue garantizar los derechos de los compradores. Asimismo, tiene como objetivo impulsar el desarrollo balanceado de las empresas del sector.
2. *La Directiva 34/2002*, a partir de la fecha 11 de julio, controla Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI). El objetivo de esta normativa se basa en crear un marco legal que impulse el desarrollo de la sociedad en línea. También, asegurará la protección legal en los tratos electrónicos y protege los derechos de los usuarios de plataformas digitales.

Por último, las mercancías que sean proporcionadas contarán con la calidad correspondiente y deben venir con las garantías necesarias. También, las medidas para llevar a cabo el reclamo, desistimiento o reembolso de los bienes deben ser igual de eficientes.

3 Metodología

La metodología que será utilizada en este trabajo busca medir el nivel de conocimiento de seguridad en el ámbito del comercio digital de las personas que realizan compras y transacciones en el internet. A través de un tipo de investigación cualitativa se pretende conocer la cantidad de conocimiento de los clientes fundamentado en los peligros y riesgos que se pueden hallar. Además, se pretende entender las precauciones que pueden elegir usar, las medidas de prevención que deben considerar durante la entrega de datos personales e informarse sobre los protocolos de seguridad que las compañías deben utilizar como organización para resguardarlos.

Esta sección de la propuesta es crucial ya que se podrá descubrir la percepción y el entendimiento de los usuarios fundamentado en la seguridad en línea y la protección de la información en las compras por internet.

Después de obtener los datos se llevó a cabo una evaluación para establecer si los clientes están conscientes de los crímenes que pueden experimentar después de efectuar una compra por internet o una transacción económica. Se ha determinado que gran parte de los consumidores no se dan cuenta de las amenazas vinculadas a estas prácticas.

3.1 Población y muestra

Para alcanzar el objetivo del estudio que estoy realizando he creado un formulario utilizando un grupo representativo de 39 participantes. Los sujetos elegidos para este análisis fueron escogidos de manera aleatoria ya que así asegura la veracidad y participación de los encuestados. De estos 39 encuestados, 23 son hombres y 16 son mujeres.

La edad de estos varía desde los 18 años hasta los 64, gracias a este rango podemos obtener una visión más amplia y detallada acerca del conocimiento de la seguridad en el comercio electrónico. Estos 39 encuestados poseen una formación académica y unos ingresos distintos entre ellos, esto no proporcionará resultados distintos y se estudiará la correlación entre varios factores.

Gracias a la participación de los entrevistados he podido obtener información en base a conocimiento, actitudes y experiencias en relación a la seguridad en el comercio online.Con esta información se podrá comprobar la preocupación de los usuarios para realizar compras por internet de forma segura y protegida.

Con esta encuesta quiero contribuir información valiosa y poder colaborar en el debate de la importancia de la seguridad en el comercio electrónico además de poder fomentar experiencias seguras y protegidas para los usuarios en el comercio digital.

3.2 Técnicas y herramientas de recolección de datos

Este estudio se basa en un tipo de estudio cualitativo para investigar y entender la visión de los encuestados sobre la seguridad en el comercio electrónico. El objetivo es recopilar los datos mediante una encuesta realizada por 39 personas. Este cuestionario incluye 16 preguntas elaboradas para obtener información específica.

La encuesta proporciona diferentes alternativas para responder y otorga a los entrevistados la libertad de elegir más de una opción cuando sea necesario. Esto posibilita una perspectiva más amplia y minuciosa de los puntos de vista y acciones de los actores acerca de la seguridad en internet.

La etapa de captura de registros se ejecuta por medio de una plataforma electrónica. En particular, se utiliza la herramienta de Google Forms, que brinda una herramienta eficiente y confiable para elaborar y adaptar este tipo de exámenes. El uso de esta herramienta tecnológica permite el fácil acceso e involucramiento de aquellos que responden a la encuesta. De forma simultánea, protege la confidencialidad y asegura los datos obtenidos.

Una de las principales ventajas de este sistema es debido a que los resultados obtenidos de las encuestas se graban automáticamente. Esto facilita considerablemente el examen y gestión de los datos. También, la plataforma de Google suministra visualizaciones gráficas y porcentajes claros y visuales. Esto posibilita una comprensión más veloz y exitosa de los informes alcanzados.

3.3 Análisis de datos

Tras la realización de los cuestionarios por la muestra elegida, se obtienen datos suficientes para determinar un resultado. Gracias a la herramienta de Google Forms, cada respuesta recibida nos proporciona una serie de porcentajes y gráficos para comparar las distintas opciones elegida por la población.

El estudio comparativo de las diferentes respuestas suministradas por los usuarios ha sido fundamental para detectar patrones y tendencias en sus decisiones. No obstante,

resulta crucial considerar que estas respuestas pueden fluctuar según el contexto y los escenarios particulares. De este modo, hemos logrado determinar qué opciones han sido las más elegidas y qué son las preferencias más habituales entre los usuarios con respecto a la seguridad en las operaciones de comercio electrónico. Los resultados obtenidos tienen un gran valor para incrementar la experiencia de compra en el mundo virtual.

Este método de recopilación y evaluación de información nos ha entregado un fundamento firme para comprender las conclusiones. Asimismo, ha posibilitado elaborar un informe que exprese de forma precisa la realización del objetivo propuesto en este proyecto. La mezcla de imágenes y cifras calculadas por la aplicación de Google Drive nos ha posibilitado observar de manera nítida y eficiente los patrones y gustos de los participantes en la encuesta.

Además, es relevante destacar que utilizar esta herramienta tecnológica ha optimizado el proceso de recolección y análisis de datos. Eso nos ha posibilitado obtener logros de forma más productiva y puntual. La comodidad de obtener los datos ha sido muy útil para realizar un estudio exhaustivo de los resultados.

4 Resultados

4.1 Análisis descriptivo de los datos

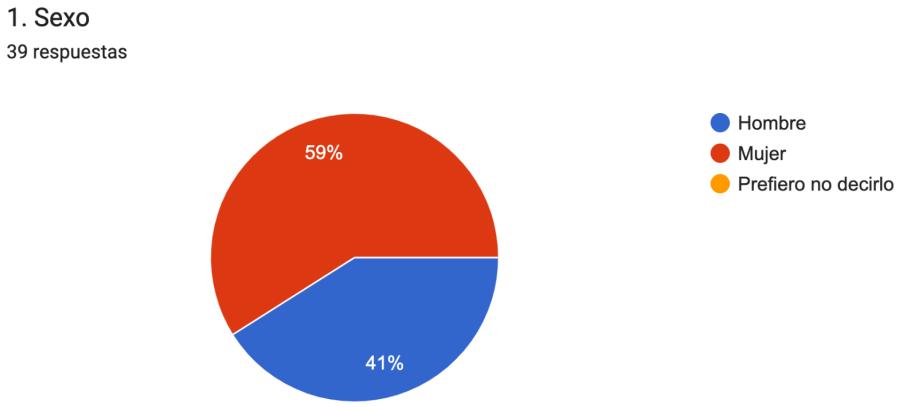

Gráfico 1: Pregunta 1 encuesta Seguridad en compras online

En este gráfico se puede ver la primera pregunta de la encuesta en la cual se pregunta a los encuestados su sexo. El 59 % son mujeres y el 41 % son hombres, por lo que la mayoría de los encuestados son mujeres.

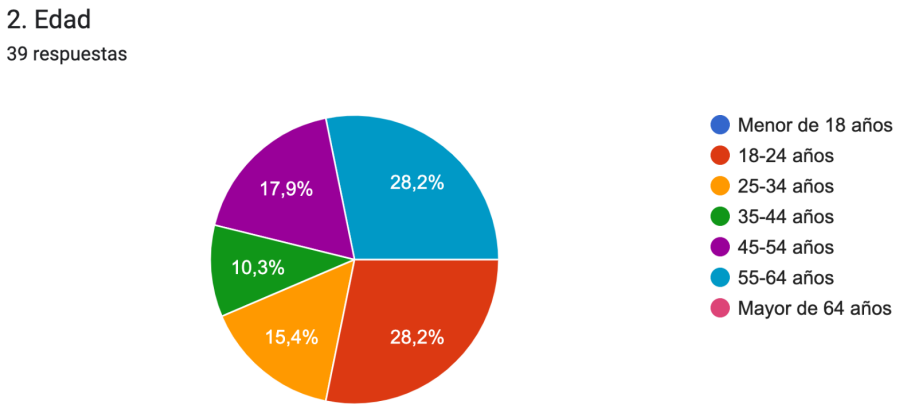

Gráfico 2: Pregunta 2 encuesta Seguridad en compras online

Podemos observar que las edades de los encuestados son muy variadas; no hay una gran mayoría ya que los porcentajes se reparten entre las distintas edades. EL 28,2 % de los encuestados tienen entre 55 y 64 años, el 28,2 % de los encuestados son jóvenes de entre 18 y 24 años, el 17,9 % pertenece a personas de entre 45 y 54 años, el 15,4 % son personas de entre 25 y 34 años y por último el 10,3 % pertenece a los encuestados que tienen entre 35 y 44 años.

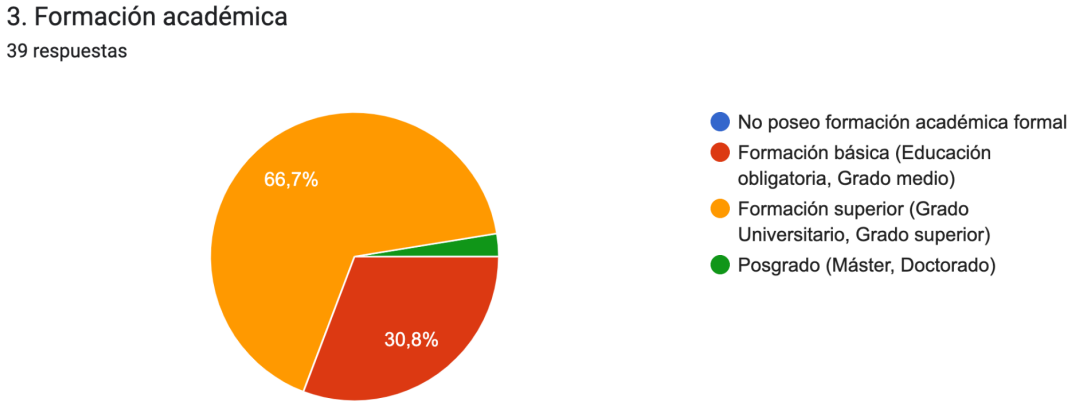

Gráfico 3: Pregunta 3 encuesta Seguridad en compras online

En la pregunta 3 del cuestionario se busca saber la formación académica de las personas encuestadas. Podemos observar que el 66,6 % han recibido una formación superior (Grados universitarios o grados superiores), el 30,8 % de ellos han recibido una

formación básica como la educación o grados medios, y por último el 2,6 % han realizado estudios postgrados como máster o doctorados.

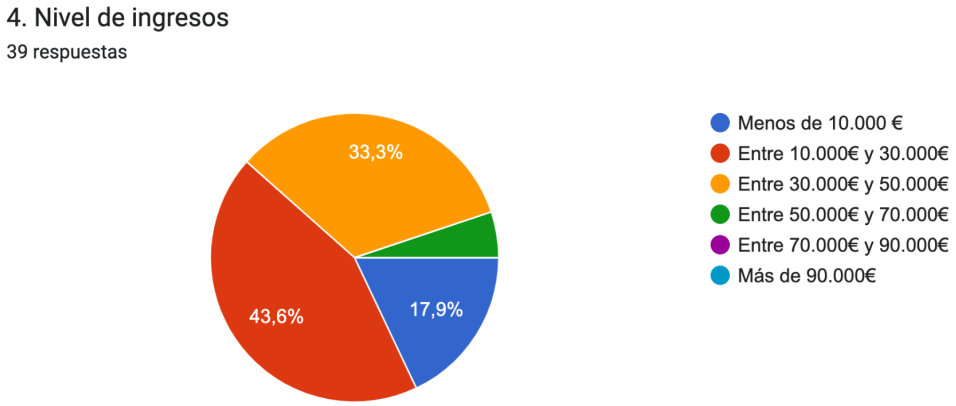

Gráfico 4: Pregunta 4 encuesta Seguridad en compras online

En la cuestión 4 se pregunta a los encuestados por su nivel de ingresos. Como podemos observar en la imagen el 43,6 % de los encuestados reciben unos ingresos anuales de entre 10.000 € y 30.000 €, el 33,3 % son aquellos encuestados que reciben anualmente entre 30.000 € y 50.000 €, el 17,9 % son personas encuestadas que reciben anualmente unos ingresos de menos de 10.000 € y el 5,1 % de los encuestados reciben al año unos ingresos de entre 50.000 € y 70.000 €.

Gráfico 5: Pregunta 5 encuesta Seguridad en compras online

En la cuestión número 5 he preguntado a los encuestados si realizan o no compras de manera online. El 97,4 %, es decir, 38 personas han respondido "·Sí" mientras que sólo un 2,6 %, 1 persona ha respondido "No".

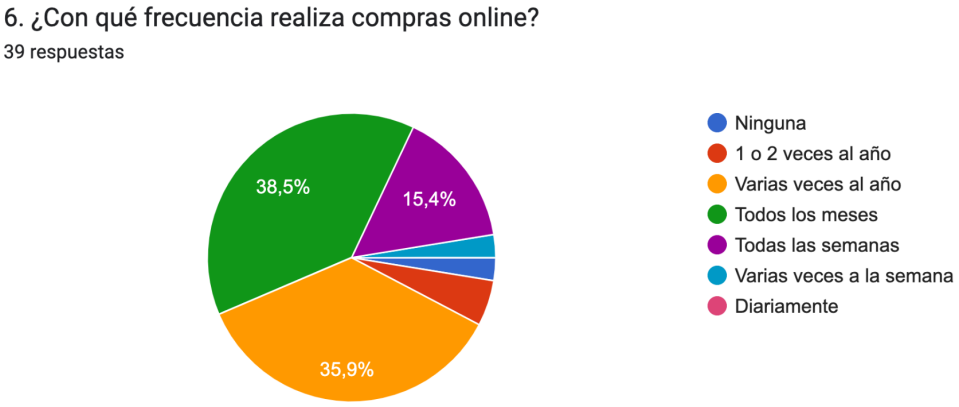

Gráfico 6: Pregunta 6 encuesta Seguridad en compras online

En la pregunta 6 del cuestionario, se ha realizado la pregunta "¿Con qué frecuencia realiza compras online?", el 38,5 % han respondido que realizan compras por internet todos los meses del año, el 35,9 % han afirmado que realizan compras online varias veces al año, el 15,4 % realizan compras todas las semanas, el 5,1 % hacen

compras por internet diariamente y por último realizan compras varias veces a la semana y ninguna vez el mismo porcentaje, un 2,6 %.

Gráfico 7: Pregunta 7 encuesta Seguridad en compras online

En la cuestión 7 el 97.4%, representado por 38 personas, ha confirmado realizar compras de manera online. Esta abrumadora mayoría refleja la creciente popularidad y aceptación del comercio electrónico en nuestra sociedad. La comodidad y la amplia variedad de opciones que ofrece el mundo digital han llevado a que casi la totalidad de los encuestados prefiere realizar sus compras desde la comodidad de sus dispositivos electrónicos.

No obstante, también es esencial destacar que el 2.6% restante, es decir, una sola persona, respondió "No" a la realización de compras en línea. Aunque este porcentaje es significativamente menor en comparación con el grupo que sí compra por internet, no podemos pasar por alto la existencia de esta minoría que prefiere otras formas de adquirir bienes y servicios.

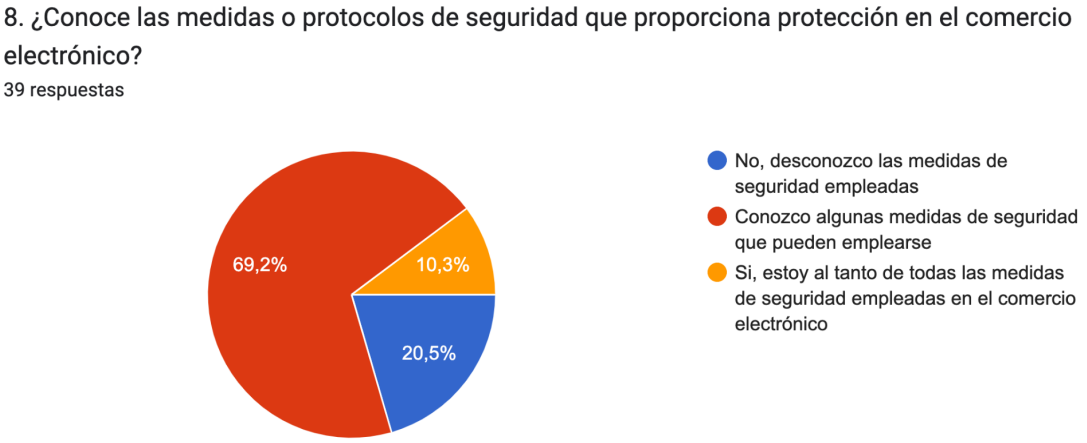

Gráfico 8: Pregunta 8 encuesta Seguridad en compras online

En la pregunta 8 de la encuesta se busca saber el conocimiento que los usuarios tienen sobre las medidas y protocolos que se usan para asegurar el comercio electrónico. El 69,2 % de los encuestados conocen alguna de las medidas de seguridad que se utiliza para proteger la compra de los consumidores, el 20,5 % de las personas encuestadas desconoce las medidas de seguridad empleadas en la protección de los usuarios y el 10,3 % conoce todas las medidas de seguridad empleadas en el comercio electrónico.

Gráfico 9: Pregunta 9 encuesta Seguridad en compras online

En la pregunta 9 se busca saber el conocimiento de los usuarios sobre las amenazas y riesgos que pueden encontrarse a la hora de realizar una compra online. El 76,9 % si son conscientes de alguna amenaza que puedan afectarles cuando realizan compras en internet. El 12,8 % conoce todas las amenazas y riesgos que pueden

afectarles y el 10,3 % no están seguros de las amenazas y riesgos que pueden afectarles en una compra online.

Gráfico 10: Pregunta 10 encuesta Seguridad en compras online

En la cuestión número 10 se pregunta la confianza del consumidor en la seguridad otorgada por las tiendas online. El 64,1 % confirma que confía en la seguridad de las tiendas, pero, aun así, buscan asegurarse una protección garantizada. El 23,1 % desconfía de la efectividad de las medidas de seguridad aportadas por la tienda online y el 12,8 % confían totalmente en la seguridad aportada a los consumidores por las tiendas online.

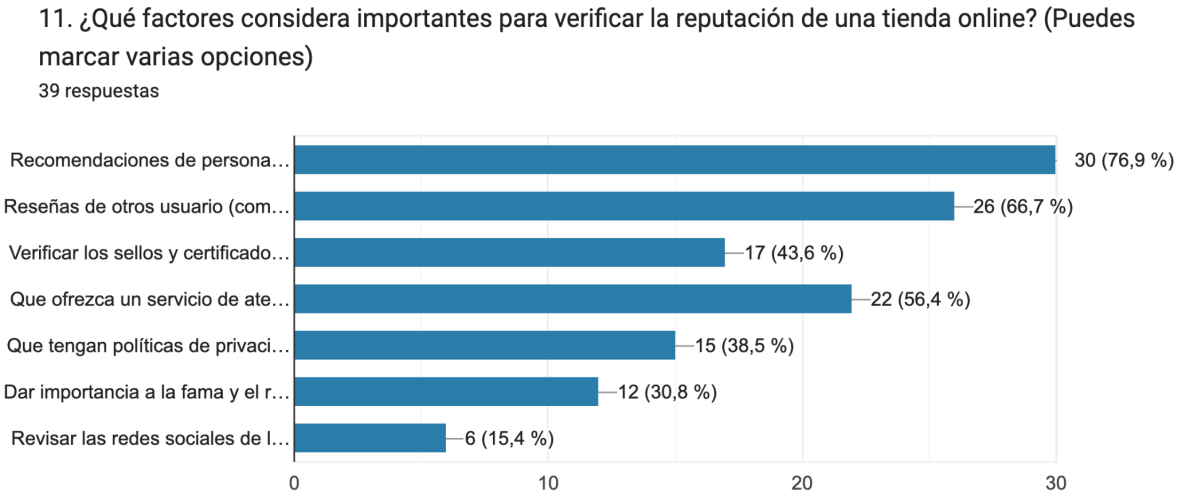

Gráfico 11: Pregunta 11 encuesta Seguridad en compras online

En la pregunta 11 se pregunta a los usuarios cuáles son los factores que consideran importantes para verificar la reputación de una tienda online. Pueden escoger varias opciones, el 76,9 % (30 elecciones) verifican la reputación de las tiendas online mediante la recomendaciones de personas que ya han comprado en estos sitios web anteriormente, el 66,7 % (26 elecciones) confían en las reseñas que otros usuarios suben para dar su opinión de su experiencia en las tiendas online, el 43,6 % (17 elecciones) buscan verificar y garantizar que las tiendas poseen sellos y certificados de calidad y seguridad, el 38,5 % (15 elecciones) quieren verificar las políticas de privacidad y protección definidas claramente, el 30,8 % (12 elecciones) de los encuestados dan importancia a la fama y reputación de las tiendas web y el 15,4 % (6 elecciones) de las personas encuestadas revisan las redes sociales de las tiendas vara garantizar su reputación y seguridad.

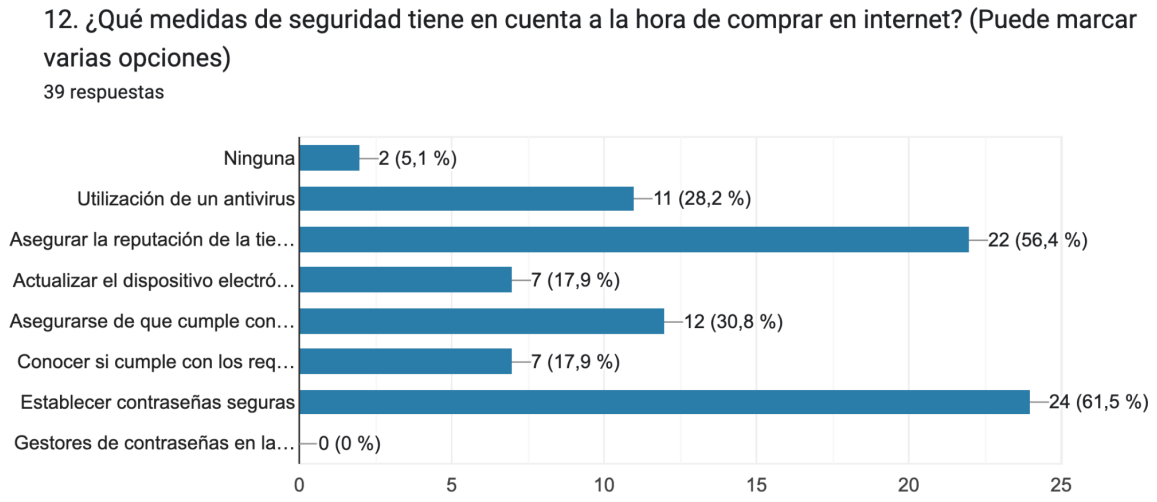

Gráfico 12: Pregunta 12 encuesta Seguridad en compras online

En la pregunta 12 se buscaba conocer las medidas de seguridad que los consumidores tienen en cuenta a la hora de comprar en internet. Pueden elegir varias opciones, el 5,1 % (2 elecciones) no tienen en cuenta ninguna medida de seguridad a la hora de realizar una compra por internet, el 28,2 % (11 elecciones) utiliza un antivirus para prevenir las amenazas y riesgos que se puedan encontrar, el 56,4 % se aseguran de la buena reputación que posee el sitio web, el 17,9 % (7 elecciones) actualiza sus dispositivos electrónicos para prevenir un fallo en la seguridad de dichos dispositivos. El 30,8 % (12 elecciones) de los encuestados se aseguran que las tiendas online cumplen con los Certificados de capa de servidor segura (SSL), el 17,9 % (7 elecciones) de las personas encuestadas buscan conocer si los sitios web donde van a realizar una compra

cumplen con los requisitos de PCI-DSS y el 0 % de los encuestados no utilizan gestores de contraseñas para garantizar la eficacia de estas.

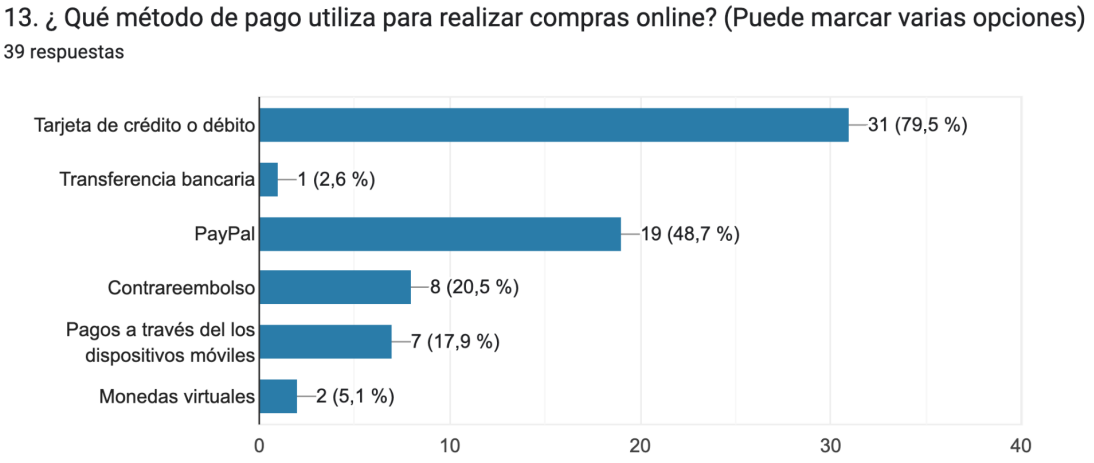

Gráfico 13: Pregunta 13 encuesta Seguridad en compras online

En la pregunta 13 del cuestionario se requería conocer el método de pago utilizado en internet por los consumidores. Podían escoger varias opciones, el 79 % (31 elecciones) pagan los productos o servicios adquiridos en internet mediante tarjeta de crédito o débito, 2,6 % (1 elección) admite pagar por transferencia bancaria, el 48,7 % (19 elecciones) de los encuestados admiten utilizar PayPal como método de pago, el 20,5 % (8 elecciones) utilizan el método de contrarrembolso, 17,9 % (7 elecciones) realizan pagos a través de los dispositivos móviles y por último el 5,1 % (2 elecciones) de los encuestados utiliza monedas virtuales para realizar pagos por internet.

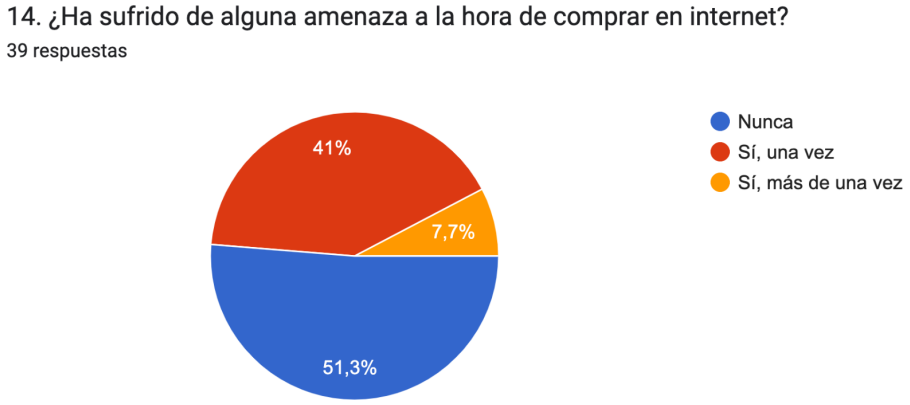

Gráfico 14: Pregunta 14 encuesta Seguridad en compras online

En la pregunta 14 se ha preguntado a los encuestados si alguna vez han sufrido algún tipo de amenaza a la hora de realizar compras en internet. El 51 % (20 elecciones) de los encuestados han respondido que nunca han padecido ninguna amenaza comprando por internet. El 41 % (16 elecciones) han respondido que han sufrido una amenaza una vez y el 7,7 % (3 elecciones) de los encuestados han respondido que han sufrido amenazas más de una vez cuando han comprado en internet.

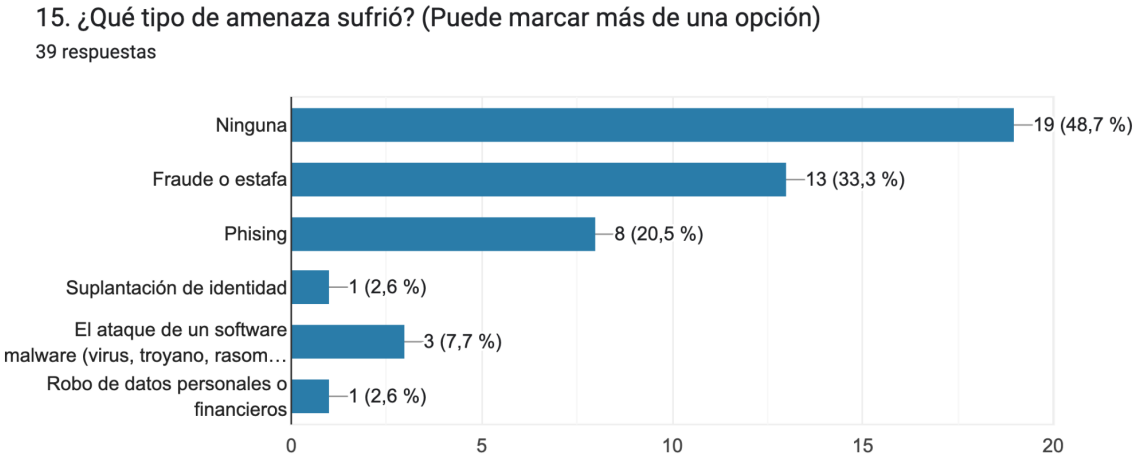

Gráfico 15: Pregunta 1 encuesta Seguridad en compras online

En la cuestión 15 se realiza la pregunta al encuestado “¿Qué tipo de amenaza sufrió?”. El 48,7 % (19 elecciones) han respondido que no han sufrido ningún tipo de amenaza, el 33,3 % (13 elecciones) de los encuestados los consumidores han sufrido algún tipo de fraude o estafa, el 20,5 % (8 elecciones) han sufrido una caso de phishing, 2,6 % (1 elección) ha respondido que fue víctima de una suplantación de identidad, el 7,7 % (3 elecciones) han sido víctimas de un ataque de un software malware (troyano, virus ransomware o keylogger) y por último el 2,6 % (1 elección) ha sufrido un robo de datos personales o financieros.

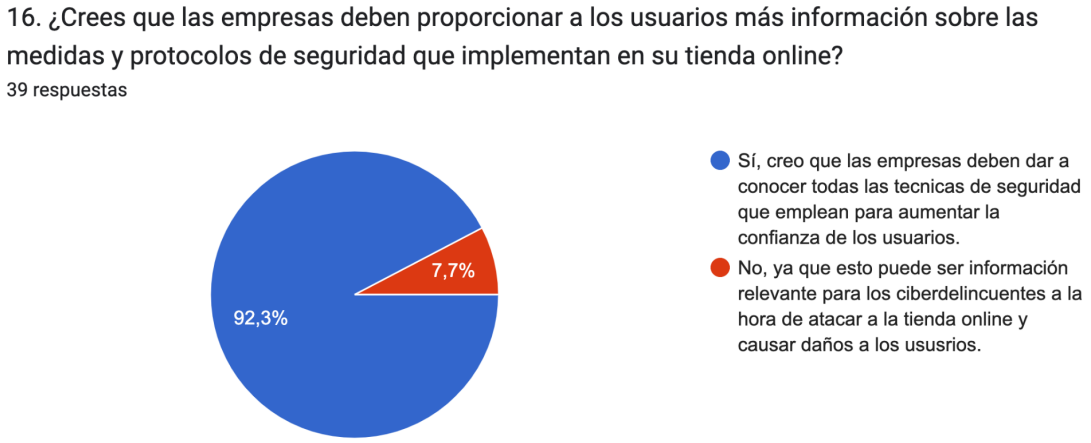

Gráfico 16: Pregunta 1 encuesta Seguridad en compras online

El 92,3 % de los participantes encuestados, que conforman la mayoría, manifestaron firmemente que las compañías deben proporcionar más detalles sobre sus precauciones de seguridad. Este enfoque demuestra una cada vez mayor conciencia en los compradores acerca de la importancia de entender cómo se resguardan sus datos personales y transacciones al efectuar compras en la web. Al aprender los métodos de seguridad utilizados, los clientes pueden sentirse más seguros y relajados cuando comparten datos personales y financieros en las plataformas de venta en internet. No obstante, vale la pena mencionar que ningún sistema de protección no es invulnerable y siempre es recomendable tomar precauciones al compartir información confidencial en internet.

Además, Alrededor del 7,7 % de los participantes indicaron su desacuerdo con la noción de que las tiendas en línea ofrecen detalles completos sobre las medidas de seguridad. Entre sus inquietudes, algunos afirmaron que divulgar estas estrategias podría

proporcionar pistas a los delincuentes informáticos. Esto quizás puede ayudar a sus comportamientos delictivos. Hay que mencionar que a pesar de que este grupo reducido no está de acuerdo con la transparencia completa, esto no significa que no vean como importante la seguridad en el comercio en internet.

4.2 Pruebas estadísticas

1. Análisis de variables Sexo / Métodos de pago

SEXO / MÉTODO DE PAGO	Tarjeta de crédito o débito	PayPal	Contrareembolso	Pagos a través del losdispositivos móviles	
Hombre	7	9	3	3	22
Mujer	22	11	5	3	41
	29	20	8	6	63

Figura 11: Análisis de variables Sexo / Métodos de pago. Fuente: Elaboración propia

Figura 12: Resultado de dependencia de las variables Sexo / Métodos de pago. Fuente: Elaboración propia

El análisis de las variables cruzadas de sexo y el método de pago ha resultado en que son variables independientes. Esto implica en que no hay una conexión importante entre el sexo de los participantes y la forma de pago empleada en las compras online.

Esto se puede dar por muchos factores, uno de ellos son las preferencias y gustos de cada persona ya que el medio de pago empleado puede llevarse a cabo por preferencias individuales de cada consumidor así también como su situación financiera y por ello no depende del género de este.

También hay que tener en cuenta los factores económicos y sociales, ya que la forma de pago puede verse afectada por diferentes factores económicos como los ingresos de cada consumidor, el contexto laboral y las preferencias de compras o el nivel educativo de cada usuario.

Además, en la nueva época digital las formas de pago han avanzado enormemente y se han presentado varias alternativas nuevas como monederos electrónicos o las monedas virtuales, esto han provocado una gran variedad en la selección del método de pago pudiendo alejar cualquier relación entre el sexo y la forma de pago.

También hay que tener en cuenta que el análisis se sustenta en una muestra de población pequeña por lo que los resultados pueden mostrar los rasgos de ese grupo en específico.

Por lo tanto, el sexo y el método de pago son variables no dependientes entre sí lo que sugiere que otras variables como las preferencias personales o los factores económicos y sociales pueden ser más significativos en esta relación.

2. Análisis de variables Ingresos/ frecuencia

INGRESOS / FRECUENCIA	Varias veces al año	Todos los meses	Todas las semanas	
Menos de 10.000 €	4	3	0	7
Entre 10.000€ y 30.000€	6	5	2	13
Entre 30.000€ y 50.000€	3	6	3	12
Entre 50.000€ y 70.000€	0	1	1	2
	13	15	6	**34**

Figura 13: Análisis de variables Ingresos / Frecuencia de compra online. Fuente: Elaboración propia

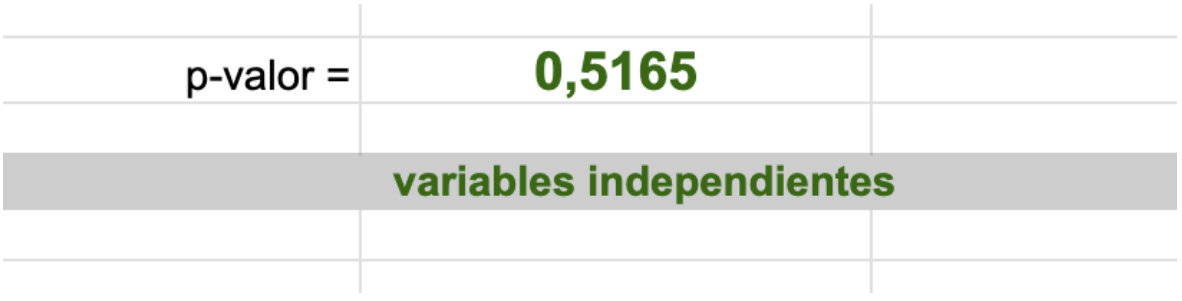

Figura 14: Resultado de dependencia de las variables Ingresos / Frecuencia de compra online. Fuente: Elaboración propia

En esta imagen podemos observar que las variables de ingresos que recibe el encuestado anualmente con la frecuencia de compras que realiza no son dependientes entre sí.

La regularidad con la que los usuarios hacen compras online podría estar más influenciada por sus gustos y necesidades personales que por los ingresos que reciben. Algunos encuestados pueden poseer un nivel adquisitivo alto pero prefieren efectuar sus compras en locales físicos mientras que puede haber encuestados que poseen un nivel adquisitivo más bajo pero prefiere comprar por internet. La forma de vida de las personas puede ser un factor muy importante a la hora de analizar la frecuencia de sus compras y no por su nivel adquisitivo.

La posibilidad de comprar por internet no es obligatoriamente un factor que esté ligado a la adquisición de bienes y servicios por internet. Las personas con un bajo nivel adquisitivo tienen acceso a internet y por ello son capaces de realizar compras online de manera regular, además, de aprovechar promociones, rebajas y descuentos que algunas tiendas solo brindan de manera digital. Por ello la cantidad de compras realizadas en la web no están necesariamente vinculadas a la capacidad económica de las personas.

También hay otros factores económicos que pueden afectar la frecuencia de compra de los consumidores, esto engloba a los fondos disponibles que tienen para realizar compras, así como las necesidades de financiamiento y las demandas personales. Estos factores pueden alejar la relación entre los beneficios y las frecuencias de compras online.

Por esta razón, se debe tomar en cuenta que el cuestionario posee un pequeño tamaño de muestra. Los hallazgos pueden revelar rasgos de los sujetos de estudio de forma precisa. El número de adquisiciones en línea no se correlaciona directamente con la capacidad de compra de los clientes. Se basan en otras variables como las elecciones personales y otros aspectos económicos que inciden en los usuarios.

3. Análisis de variables formación académica/ conocimiento de medidas de seguridad

FORMACIÓN / CONOCIMIENTO MEDIDAS DE SEGURIDAD	No, desconozco las medidas de seguridad empleadas	Conozco algunas medidas de seguridad que pueden emplearse	Si, estoy al tanto de todas las medidas de seguridad empleadas en el comercio electrónico	
Formación básica (Educación obligatoria, Grado medio)	5	8	0	13
Formación superior (Grado Universitario, Grado superior)	3	19	4	26
	8	27	4	39

Figura 15: Análisis de variables Formación académica / Conocimiento medidas de seguridad. Fuente: Elaboración propia

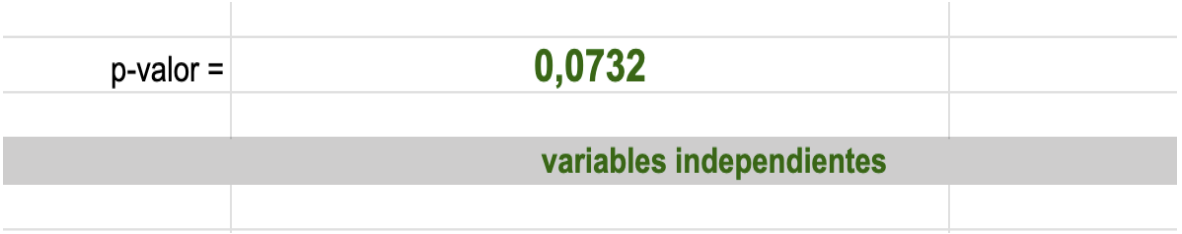

Figura 16: Resultado de dependencia de las variables Formación académica / Conocimiento medidas de seguridad. Fuente: Elaboración propia

En la anterior imagen podemos observar un análisis de variantes cruzadas en la formación académica del encuestado y el conocimiento que este posee sobre medidas de seguridad. Como bien indica el análisis estas variables son independientes entre sí.

Esto puede darse por varios factores como que el conocimiento de las medidas de seguridad, pueden adquirirse gracias al acceso a la información en internet que tienen a su alcance los usuarios, aunque dicho conocimiento necesita de una educación base formal, la disponibilidad de datos y la capacidad de aprendizaje del usuario puede afectar a la comprensión y entendimiento de medidas y protocolos de seguridad.

Otro factor que puede afectar a este análisis son los gustos e intereses personales de cada usuario, ya que si muestra un interés por la seguridad en el comercio electrónico puede adquirir mayor conocimiento gracias a la motivación personal. Por ello este conocimiento adquirido sin formación específica puede diferir entre los participantes, aunque no esté directamente relacionado con la formación académica.

También hay que tener en cuenta la experiencia práctica de los usuarios ya que al realizar compras por internet pueden haberse enfrentado a diversas amenazas y riesgos y aprender de estas situaciones pudiendo identificar a tiempo un posible fraude o estafa.

En este análisis puede haber otros factores que indiquen que la formación académica y el conocimiento de las medidas de seguridad en el comercio electrónico cómo la curiosidad, la conciencia de cada individuo sobre la ciberseguridad o la preocupación individual de ser víctima de un ciberdelito.

Por ello, las medidas de seguridad en el comercio electrónico son variables no dependientes de la formación académica de los encuestados, factores como los

intereses, el acceso a información relativa a la seguridad online y la experiencia de los usuarios pueden producir este resultado.

4. Análisis de variable caso de ciberdelito sufrido / frecuencia de compras online

CASO CIBERDELITO SUFRIDO / FRECUENCIA DE COMPRAS ONLINE	Varias veces al año	Todos los meses	Todas las semanas	
Nunca	9	6	3	18
Sí, una vez	2	8	3	13
	11	14	6	31

Figura 17: Análisis de variables caso ciberdelito sufrido / Frecuencia de compras online. Fuente: Elaboración propia

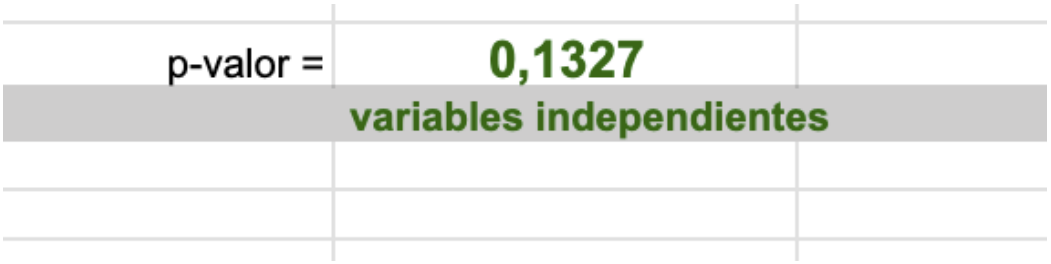

Figura 18: Resultado de dependencia de las variables caso ciberdelito sufrido / Frecuencia de compras online. Fuente: Elaboración propia

En la imagen anterior podemos observar que, tras hacer un análisis de variables cruzadas, casos de ciberdelito sufridos y la frecuencia de compras online, podemos determinar que son independientes entre sí.

Esta independencia se puede basar en que el haber experimentado un ciberdelito puede estar influenciado por diversos factores como la protección de datos personales, el tipo de actividad realizada en internet o la visita a páginas web no seguras y con alto riesgo de contener un software malicioso. Por ello cada usuario está expuesto a amenazas o riesgos sin importar la frecuencia con la que realiza compras en internet.

También la experiencia es un factor importante a la hora de ser víctima de un ciberdelito ya que haber vivido una situación similar da como resultado ser un usuario más precavido y reducir el riesgo de sufrir un ataque. Por este motivo no depende de la cantidad de compras que se hagan por internet si no ser conscientes de estas amenazas y prevenirlas lo máximo posible.

No utilizar contraseñas seguras, navegar en lugares protegidos, actualizar el software y tener un conocimiento básico de ciberseguridad son factores que afectan a la posibilidad de ser víctima de un ciberdelito por ello no depende de la frecuencia de compra.

Hay que tener en cuenta que el tamaño de la muestra recogida es pequeña, y que los resultados pueden mostrar las características de dicho grupo en específico.

Por ello la experiencia de haber sufrido un ciberdelito es una variable independiente de la frecuencia con la que se realiza compras por internet por lo que podemos deducir que dependen de otros factores.

4.3 Interpretación de resultados

La investigación llevada a cabo sobre la protección en compras en línea ha suministrado detalles útiles para el análisis por medio de los participantes encuestados. La magnitud del estudio realizado por el sondeo fue de 39 individuos. De los encuestados 23 son mujeres y 16 son hombres, si hablamos de la edad nos encontramos porcentajes similares.

La mayoría de los participantes en la encuesta contaban con un nivel educativo alto (66,6%), esto comprende títulos universitarios o estudios superiores. El 38% disponían de una educación básica, mientras que el 2,6% habían cursado estudios de postgrado. Las tasas de los grados de compra son muy similares. El 43,6 % reciben salarios de entre 10.000 € y 30.000 € y el 33,3 % de los encuestados tienen sueldos anuales de 30.000 € a 50.000 €.

Casi el 98% de aquellos que fueron encuestados hacen compras en línea. El 38,5 % hacen compras cada mes y el 35,9 % efectúan diversas compras durante el año. Gracias a la información obtenida se ha estimado un resultado favorable con respecto a la seguridad en el comercio electrónico ya que un 94,9 % ha considerado un factor importante a la hora de realizar compras online.

El 69,2 % de las personas encuestadas saben de alguna de las reglas usadas para garantizar la seguridad en las compras por internet mientras que aproximadamente el 20 % no tiene conocimiento sobre estas medidas.

La mayoría de los entrevistados, el 76,6 % conocen las amenazas y riesgos que pueden perjudicarlos a la hora de comprar por internet aun así algunos de los entrevistados no realizan prevenciones para comprar de manera segura.

El 64,1 % de los encuestados confían en la seguridad ofrecida por las tiendas web pero aun así toman precauciones. El estudio realizado referente a la seguridad en compras en línea ha brindado detalles importantes para el estudio. El tamaño de la investigación efectuada por la encuesta se realizó con 39 sujetos. De estas, 23 mujeres han sido (59 %) y 16 hombres (41 %). Las tasas son iguales entre los adolescentes de 18 a 24 años inclusive y los seres humanos de 55 a 64 años de vida.

La gran parte de los involucrados en el estudio tenían un alto nivel de educación (66,6%). Esto abarca grados universitarios o educación avanzada. El 38 % tenían educación primaria, aunque el 2,6 % por ciento habían realizado estudios de posgrado. Los valores de las categorías de adquisición son extremadamente parecidos. Un 43,6 % reciben ingresos cada año que oscilan entre 10.000 € y 30.000 € y el 33% de los encuestados obtienen ingresos anuales en el rango de 30.000 € a 50.000 €.

El 98 % de los encuestados efectúan compras en por internet. El 38,5 % compran todos los meses y 35,9 % realizan diferentes adquisiciones a lo largo de todo el año.

5 Discusión

En este apartado se realizará una observación externa sobre el proceso de realización del trabajo, así como las conclusiones que se han obtenido debido a los resultados hallados en el tipo de estudio empleado. En los apartados siguientes se examinará de qué forma los resultados guardan una relación con el conocimiento de los usuarios sobre la seguridad en el comercio electrónico.

En las limitaciones del estudio se identificarán y analizarán los problemas que han aparecido durante el avance de este estudio. Como las limitaciones de la muestra, problemas en la metodología y otros aspectos que han influido en la obtención de resultados. También se expondrá en el apartado de recomendaciones para futuras investigaciones ciertos consejos y orientaciones para las futuras investigaciones de este ámbito (seguridad en el comercio electrónico) que se vayan a realizar.

Por ello en este apartado se analizará de manera teórica los resultados prácticos y teóricos de este trabajo destacándose importancia de la seguridad en el comercio electrónico para los consumidores y empresas.

5.1 Limitaciones del estudio

Aunque se haya conseguido recoger información y resultados importantes para la

investigación es crucial dar a conocer las barreras e inconvenientes que me he encontrado al realizar este estudio.

Uno de estos inconvenientes fue el tamaño de la muestra. Al ser de 39 personas puede considerarse un tamaño de muestra bastante reducido y puede interferir en los resultados. Una muestra más grande para este tipo de estudio podría haber sido más efectiva a la hora de suministrar datos más precisos y con mayor peso.

La muestra fue elegida aleatoriamente por lo que algunos grupos de encuestados pueden no estar correctamente representados en la investigación. Esto puede influir en la representatividad y en la validez de la información obtenida.

También puede haber la posibilidad de que los participantes de la encuesta podrían haber dado respuestas socialmente correctas o incorrectas debido a que no recordasen con exactitud, no entendiesen la pregunta o no comprendiesen las respuestas ofrecidas. Por ello creo que es un factor importante considerar que estos errores pueden influir en el resultado obtenido.

La mayoría de las encuestas se realizaron en una zona geográfica en concreta por lo que puede haber causado interpretaciones sesgadas o ambiguas.

A pesar de estas limitaciones, la investigación ofrece una visión sobre las opiniones y acciones que los consumidores toman cuando realizan compras por internet. Pero aun así es necesario tener en cuenta dichas limitaciones para interpretar los resultados y aplicar los datos obtenidos.

5.2 Recomendaciones para futuras investigaciones

Tras haber realizado el tipo de estudio mostrado anteriormente y haber obtenido los resultados a continuación se va a mostrar diferentes factores que pueden ayudar a futuras investigaciones sobre la seguridad de las compras online.

Cuando se lleva a cabo la modalidad de investigación, se sugiere ampliar la recolección de datos y emplear una muestra de mayor tamaño. Esta medida permitirá conseguir datos más rigurosos. Cuando se lleva a cabo la investigación con una muestra más grande es posible conseguir una visión más exacta de las percepciones, actitudes y conductas de los clientes con respecto a la seguridad en las compras por internet. No obstante, resulta crucial considerar que el incremento en el tamaño del conjunto de datos también puede llevar consigo un costo más elevado y el tiempo requerido para recolectar

los datos. Sin embargo, hay que tener en cuenta que recoger datos de un tamaño de muestra mayor también puede necesitar más dedicación y tiempo.

Es recomendable tener una muestra de diferentes localidades geográficas ya que el comportamiento y las actitudes de pueden variar según las zonas geográficas, este factor podría afectar a la manera en la que los usuarios adquieren bienes y servicios en las tiendas web y en las medidas que toman para proteger la transacción económica. Algunas zonas podrían tener normas más rigurosas y sistemas de seguridad más sofisticados además las opiniones y creencias culturales también pueden modificar la confianza del consumidor en el comercio electrónico. Según la cantidad en la que se lleva a cabo compras online en distintos sitios pueden influir en la confiabilidad de los clientes.

En sitios donde se llevan a cabo pocas adquisiciones, la seguridad que sienten los residentes en la confianza en el comercio digital es reducida. Aunque en sitios donde existen un mayor número de compras en línea, la confianza es mayor en las medidas de protección. Por esa razón factores como los estándares de seguridad, las tradiciones culturales y el acceso a internet pueden influir en la seguridad percibida por los clientes y en la confiabilidad de las transacciones electrónicas.

Es aconsejable enriquecer este estudio cualitativo como entrevistas o debates. Esta función permite alcanzar un entendimiento más profundo de las perspectivas y vivencias de los clientes. Analizar el conocimiento y la educación previa sobre ciberseguridad que los consumidores poseen antes de realizar el tipo de estudio puede ayudar a que el investigador realice tipos de estudios como entrevistas o encuestas con preguntas más precisas.

Con estas recomendaciones las futuras investigaciones podrán adquirir nuevas perspectivas y visiones y obtener resultados más precisos y con mayor veracidad fomentando la seguridad en el comercio electrónico y proteger a los consumidores.

6 Conclusión

En conclusión, con este trabajo se ha profundizado en el tema de la protección en el ámbito del comercio por internet enfocándose en el conocimiento sobre de seguridad online que poseen los consumidores al efectuar compras a través de la web. Mediante un cuestionario exhaustivo, se han obtenido datos valiosos acerca de la forma en que los usuarios perciben y se comportan en esta esfera.

La mayoría absoluta de los usuarios consultados perciben que hay peligros y

amenazas relacionados con el comercio en línea. Algunos incluso saben acerca de las precauciones de las medidas de seguridad aplicadas para resguardarlos.

Además, se encontraron zonas donde las personas deben aumentar su conocimiento de ciberseguridad ya que una parte importante de personas entrevistadas no comprende las políticas de protección usadas en las compras por internet. Esto muestra la urgencia de un mayor conocimiento y concienciación en este tema.

Aunque el conocimiento general sobre la importancia de la protección en las compras online, muchos individuos han padecido riesgos a la hora de hacer compras online. También resulta crucial considerar que el aprendizaje y la sensibilización son esenciales para evitar cualquier tipo de engaño o hurto de datos. A pesar de eso, es importante tener presente que la protección en línea es deber de todos. Esto resalta la trascendencia de fortalecer las medidas de seguridad tanto de los adquirentes como de las corporaciones. También, es esencial impulsar la sensibilización acerca de la seguridad de la información personal y promover comportamientos adecuados en el control de datos privados.

Tomando como base los hallazgos, se puede realizar varias recomendaciones para estudios y operaciones de negocio que se lleven a cabo en adelante. Es crucial estimular programas educativos dirigidos a los clientes. Estos proyectos posibilitaron adquirir un conocimiento profundo sobre las acciones de seguridad y desarrollar destrezas para detectar las amenazas y riesgos actuales.

Por eso, las empresas deben ofrecer información clara y transparente que están vinculadas a los mecanismos de protección que implementan para asegurar a sus clientes. Además, la información debe ser accesible fácilmente para que los usuarios puedan hacer elecciones con conocimiento en relación a la fiabilidad que depositan en la entidad. De esta manera, las personas pueden tomar decisiones bien fundamentadas y creer en la defensa de sus transacciones financieras. Este aspecto provocará confianza en los clientes y motivará la realización de compras online.

7 Referencias bibliográficas

ACRONIS. (2021). *¿Qué es el software antimalware y cómo funciona?* https://acortartu.link/1wq3a

appendweb. (2020). *La historia del comercio electrónico: origen y evolución.* https://acortartu.link/3km19

Avast. (2021). *¿Qué es un malware troyano? Guía definitiva.* (Belcic, 2021) https://acortartu.link/l7q5t

BBVA. (2023). *¿Qué es el phishing y cuáles son sus consecuencias?* https://acortartu.link/jtfkf

BLOGJETCOMPUTER. (2022). *Qué es un firewall o cortafuegos y cómo protege tus dispositivos.* https://acortartu.link/89566

COE. (2015). *Legislación del Comercio Electrónico.* https://acortartu.link/a08pz

Commercerentable. (2022). *¿Conoces los diferentes tipos de comercio electrónico y ecommerce?* https://acortartu.link/u6q5c

ComputerWeekly. (2012). *Los 12 requisitos PCI DSS.* https://acortartu.link/qzgou

Cyberclick. (2023). *¿Qué es un ecommerce? Tipos, cómo crearlo y ejemplos.* https://acortartu.link/0wf47

EALDE. (2020). *Qué es la norma ISO 27001 y para qué sirve.* https://acortartu.link/xolsj

EmpresaActual. (2020). *Historia y evolución del comercio electrónico.* https://acortartu.link/yvrra

GlobalSuite. (2023). *¿Qué es la norma ISO 27001 y para qué sirve?* https://acortartu.link/6jhon

Hackmetrix. (2021a). *PCI DSS: Los 12 requisitos [Parte 1].* (Araujo, 2021). https://acortartu.link/lmv4y

Hackmetrix. (2021b). PCI DSS: Los 12 requisitos [Parte 2]. (Araujo, 2021) https://acortartu.link/395q9

INCIBE. (2015). *Ciberseguridad en comercio electrónico. Una aproximación para el empresario.* https://acortar.link/9emXND

INCIBE. (2020). *Consideraciones de seguridad para tu comercio electrónico.* https://acortartu.link/3xah9

INCIBE. (2021a). *Adware.* https://acortartu.link/c3all

INCIBE. (2021b). *¿Qué es el ransomware?* https://acortartu.link/y86or

Marketing E Commerce Digital Content. (2018). *Qué es PCI DSS y por qué es imprescindible para tu eCommerce.* https://acortartu.link/t73il

Ministerio de Consumo. (2023). Regulación del comercio electrónico https://acortartu.link/ilxp8

PCI Hispano. (2022). *¿Qué es PCI SSF / PCI Secure SLC / PCI S3?* https://acortartu.link/zmd4m

Policía Nacional. (2020) *Compra segura en internet. Fichas prácticas.* https://acortartu.link/tnv1s

RedesZone. (2023). *Cómo funciona un keylogger y cómo evitarlo en Windows.* https://acortartu.link/4w2vc

Xataka. (2020). *Malware: qué es, qué tipos hay y cómo evitarlos.* https://acortartu.link/2uwdf

8 Anexo 1: Glosario

Actualización de software. Proceso de ejecutar las correcciones más actualizadas y mejoras brindadas por los ingenieros de software. La meta consiste en mantener las infraestructuras al día y seguros frente a fallos de seguridad conocidos.

Amenazas cibernéticas. Se refiere a todo tipo de acción o suceso con intenciones dañinas que busca afectar la integridad de los equipos de computación. Varios casos de este tipo de ataques contienen software malicioso, el robo de identidad en línea y el cifrado de archivos.

Autenticación. Método utilizado para validar la veracidad de una persona. Por lo general se hace mediante la mezcla de identificaciones como contraseñas, códigos o impresiones dactilares.

Ciberseguridad. Se trata del conjunto de estrategias y técnicas para proteger las computadoras y la información de potenciales riesgos e intrusiones en el contexto digital.

Comercio electrónico. Igualmente reconocido como ecommerce, hace referencia al acto de comprar y comercialización de mercancías y ayuda usando la web.

Encriptación. Método empleado para encriptar datos de forma que solo se pueda comprender por las personas que tienen la clave de desencriptación pertinente. Esto ofrece privacidad y protección a la información.

Firewall. Es una plataforma de protección que supervisa la transferencia de datos, autorizando o impidiendo determinados tipos de conexiones según pautas predeterminadas. El propósito principal consiste en asegurar la red para prevenir accesos no permitidos.

Phishing. Método empleado por los criminales informáticos para conseguir datos sensibles, como contraseñas o datos de tarjetas de crédito. Fingen ser organizaciones auténticas por medio de mensajes electrónicos de estafa.

Protección de datos. Grupo de acciones y métodos empleadas para asegurar que los datos personales y financieros de los usuarios se archive y trate de forma segura, protegiendo la privacidad y acatando las normativas y normas necesarias.

Seguridad informática. Grupo de tácticas y técnicas creadas para proteger los datos y los sistemas de ordenadores de peligros. Esto abarca la entrada sin autorización, la sustracción de información y los asaltos cibernéticos.

Anexo 2: Excel con las respuestas del cuestionario

Marca temporal	1. Sexo	2. Edad	3. Formación académica	4. Nivel de ingresos	5. ¿Realiza o ha realizado compras online?	6. ¿Con qué frecuencia realiza compras online?	7. ¿Cree que la seguridad en las c	8. ¿Conoce las medidas o protocolos de seguridad que proporciona protección en el comercio electrónico?
7/8/2023 18:25:22	Mujer	55-64 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:28:02	Mujer	45-54 años	Formación básica (Educación	Entre 10.000€ y 30.000€	No	Ninguna	No, considero que no es un factor	No, desconozco las medidas de seguridad empleadas
7/8/2023 18:33:55	Prefiero no decirlo	55-64 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:34:21	Mujer	35-44 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Todos los meses	Sí, es un factor importante para m	Sí, estoy al tanto de todas las medidas de seguridad empleadas en el comercio electrónico
7/8/2023 18:35:08	Mujer	18-24 años	Formación superior (Grado	Entre 10.000€ y 30.000€	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:36:54	Mujer	35-44 años	Formación básica (Educación	Entre 30.000€ y 50.000€	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:37:29	Mujer	55-64 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:38:39	Hombre	45-54 años	Formación básica (Educación	Entre 10.000€ y 30.000€	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:39:13	Hombre	55-64 años	Formación superior (Grado	Entre 10.000€ y 30.000€	Sí	1 o 2 veces al año	Sí, es un factor importante para m	Sí, estoy al tanto de todas las medidas de seguridad empleadas en el comercio electrónico
7/8/2023 18:40:30	Hombre	45-54 años	Formación básica (Educación	Entre 30.000€ y 50.000€	No	Ninguna	No, considero que no es un factor	No, desconozco las medidas de seguridad empleadas
7/8/2023 18:40:46	Hombre	55-64 años	Formación superior (Grado	Entre 50.000€ y 70.000€	Sí	Todas las semanas	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:41:34	Mujer	55-64 años	Formación básica (Educación	Entre 10.000€ y 30.000€	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:41:47	Hombre	45-54 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Todas las semanas	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 18:42:51	Mujer	55-64 años	Formación superior (Grado	Entre 50.000€ y 70.000€	Sí	Todos los meses	Sí, es un factor importante para Sí,	estoy al tanto de todas las medidas de seguridad empleadas en el comercio electrónico
7/8/2023 18:50:44	Mujer	55-64 años	Formación básica (Educación	Entre 10.000€ y 30.000€	Sí	1 o 2 veces al año	Sí, es un factor importante para N	No, desconozco las medidas de seguridad empleadas
7/8/2023 18:55:29	Hombre	55-64 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Todas las semanas	Sí, es un factor importante para N	No, desconozco las medidas de seguridad empleadas
7/8/2023 19:48:33	Mujer	18-24 años	Formación básica (Educación	Menos de 10.000 €	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 19:52:31	Mujer	18-24 años	Formación superior (Grado	Menos de 10.000 €	Sí	Varias veces al año	Sí, es un factor importante para N	No, desconozco las medidas de seguridad empleadas
7/8/2023 20:31:48	Hombre	18-24 años	Formación superior (Grado	Menos de 10.000 €	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 20:47:14	Mujer	45-54 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 20:49:47	Mujer	55-64 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 21:01:49	Hombre	55-64 años	Formación superior (Grado	Entre 10.000€ y 30.000€	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 21:02:49	Mujer	45-54 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Todos los meses	Sí, es un factor importante para Sí,	estoy al tanto de todas las medidas de seguridad empleadas en el comercio electrónico
7/8/2023 21:09:21	Mujer	45-54 años	Formación superior (Grado	Entre 30.000€ y 50.000€	Sí	Todas las semanas	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 21:27:28	Mujer	18-24 años	Formación superior (Grado	Menos de 10.000 €	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 21:32:03	Mujer	18-24 años	Formación superior (Grado	Menos de 10.000 €	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 21:33:26	Mujer	55-64 años	Formación superior (Grado	Entre 10.000€ y 30.000€	Sí	Varias veces a la semana	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 22:12:51	Mujer	45-54 años	Formación básica (Educación	Entre 10.000€ y 30.000€	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 22:22:09	Mujer	18-24 años	Formación superior (Grado	Menos de 10.000 €	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/7/2023 9:35:16	Hombre	25-34 años	Formación superior (Grado	Entre 10.000€ y 30.000€	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/7/2023 12:37:40	Mujer	25-34 años	Formación superior (Grado	Entre 10.000€ y 30.000€	Sí	Todos los meses	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/7/2023 13:21:27	Mujer	35-44 años	Formación básica (Educación	Entre 10.000€ y 30.000€	Sí	Todos los meses	Sí, es un factor importante para N	No, desconozco las medidas de seguridad empleadas
7/7/2023 18:29:24	Mujer	18-24 años	Formación superior (Grado	Entre 10.000€ y 30.000€	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/7/2023 18:31:01	Mujer	35-44 años	Formación básica (Educación	Entre 30.000€ y 50.000€	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/7/2023 18:58:59	Hombre	55-64 años	Formación básica (Educación	Entre 10.000€ y 30.000€	Sí	Varias veces al año	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/8/2023 0:25:40	Mujer	18-24 años	Formación superior (Grado	Entre 10.000€ y 30.000€	Sí	Todas las semanas	Sí, es un factor importante para m	Conozco algunas medidas de seguridad que pueden emplearse
7/11/2023 16:43:34	Hombre	18-24 años	Formación superior (Grado	Menos de 10.000 €	Sí	Varias veces al año	Sí, es un factor importante para N	No, desconozco las medidas de seguridad empleadas
7/11/2023 16:51:41	Hombre	25-34 años	Formación básica (Educación	Entre 10.000€ y 30.000€	Sí	Todas las semanas	No, considero que no es un factor	Conozco algunas medidas de seguridad que pueden emplearse
7/11/2023 19:46:46	Hombre	25-34 años	Formación básica (Educación	Entre 10.000€ y 30.000€	Sí	Varias veces al año	Sí, es un factor importante para N	No, desconozco las medidas de seguridad empleadas

9. ¿Es consciente de la 10. ¿ Confías en la segu	11. ¿Qué factores consid	12. ¿Qué medidas de se	13. ¿ Qué método de pa	14. ¿Ha sufrido de algun	15. ¿Qué tipo de amenaz	16. ¿Crees que las empresas deben proporcionar a los usuarios más información sobre las medidas y protocolos de seguridad que implementan en su tienda online?
Sí, soy consciente de alg	No, desconfío de la efect	Dar importancia a la fam	Asegurar la reputación d	PayPal	Ninguna	Ninguna	No, ya que esto puede ser información relevante para los ciberdelincuentes a la hora de atacar a la tienda online y causar daños a los usuarios.
Sí, soy consciente de alg	No, desconfío de la efect	Reseñas de otros usuari	Ninguna	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Verificar los sellos y certi	Utilización de un antivirus	Transferencia bancaria, (	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, conozco todas las arr	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	PayPal	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Utilización de un antivirus	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Utilización de un antivirus	Tarjeta de crédito o débi	Nunca	Ninguna	No, ya que esto puede ser información relevante para los ciberdelincuentes a la hora de atacar a la tienda online y causar daños a los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Reseñas de otros usuari	Utilización de un antivirus	Tarjeta de crédito o débi	Sí, una vez	El ataque de un software	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	No, desconfío de la efect	Recomendaciones de pe	Asegurarse de que cump	Tarjeta de crédito o débi	Sí, una vez	Phising	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, conozco todas las arr	Sí, aun así me aseguro d	Recomendaciones de pe	Utilización de un antivirus	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa, Phising	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
No estoy completamente	No, desconfío de la efect	Que ofrezca un servicio (	Ninguna	Pagos a través del los di	Nunca	Ninguna	No, ya que esto puede ser información relevante para los ciberdelincuentes a la hora de atacar a la tienda online y causar daños a los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Utilización de un antivirus	Monedas virtuales	Sí, una vez	Fraude o estafa, Phising	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, confío totalmente en l	Recomendaciones de pe	Utilización de un antivirus	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Actualizar el dispositivo t	Tarjeta de crédito o débi	Sí, una vez	Phising	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, conozco todas las arr	Sí, aun así me aseguro d	Verificar los sellos y certi	Actualizar el dispositivo t	Tarjeta de crédito o débi	Sí, más de una vez	Fraude o estafa, Phising	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
No estoy completamente	Sí, confío totalmente en l	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	No, desconfío de la efect	Recomendaciones de pe	Asegurar la reputación d	PayPal	Nunca	Phising	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, confío totalmente en l	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Reseñas de otros usuari	Asegurar la reputación d	PayPal	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	No, desconfío de la efect	Recomendaciones de pe	Utilización de un antivirus	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Reseñas de otros usuari	Asegurar la reputación d	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Dar importancia a la fam	Asegurar la reputación d	PayPal	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, conozco todas las arr	Sí, aun así me aseguro d	Verificar los sellos y certi	Asegurarse de que cump	Tarjeta de crédito o débi	Sí, una vez	Phising	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Verificar los sellos y certi	Establecer contraseñas t	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, confío totalmente en l	Recomendaciones de pe	Establecer contraseñas t	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Utilización de un antivirus	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	No, desconfío de la efect	Recomendaciones de pe	Establecer contraseñas t	PayPal	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Utilización de un antivirus	Tarjeta de crédito o débi	Sí, más de una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Utilización de un antivirus	Tarjeta de crédito o débi	Sí, más de una vez	El ataque de un software	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	No, desconfío de la efect	Recomendaciones de pe	Establecer contraseñas t	Tarjeta de crédito o débi	Sí, una vez	Fraude o estafa	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	No, desconfío de la efect	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Establecer contraseñas t	PayPal	Nunca	Ninguna	No, ya que esto puede ser información relevante para los ciberdelincuentes a la hora de atacar a la tienda online y causar daños a los usuarios.
Sí, soy consciente de alg	Sí, aun así me aseguro d	Recomendaciones de pe	Asegurar la reputación d	Tarjeta de crédito o débi	Nunca	Ninguna	Sí, creo que las empresas deben dar a conocer todas las técnicas de seguridad que emplean para aumentar la confianza de los usuarios.